THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 1:96CV01285 (RCL)**
	)	**(Alan L. Balaran, Special Master)**
GALE A. NORTON, Secretary of the Interior, et al.	)	
	)	
	)	
Defendants.	)	
	)	

REPORT AND RECOMMENDATION OF THE SPECIAL MASTER REGARDING THE SECURITY OF TRUST DATA AT THE DEPARTMENT OF THE INTERIOR

REDACTED VERSION

Table of Contents

I. INTRODUCTION

On May 17, 2001, plaintiffs filed a Consolidated Motion for an Emergency Temporary Restraining Order and Motion for a Preliminary Injunction and Motion for Order to Show Cause Why Secretary Norton, Her Employees and Counsel Should Not Be Held In Contempt ("Motion for Emergency TRO").[1] Plaintiffs' Motion[2] followed the April 2001 publication of Government Executive magazine in which then-Bureau of Indian Affairs ("Bureau" or "BIA") Chief Information Officer

---

[1] Plaintiffs are alarmed "because individual Indian trust funds and individual Indian trust records – held or created in systems managed and administered by the BIA Office of Information Resources Management ("OIRM") – have been destroyed in violation of this Court's orders or remain at risk of imminent and catastrophic loss and destruction." Motion for Emergency TRO at 1. Plaintiffs specifically asked the Court to order "government officials and their contractors to "cease the destruction of IIM-related trust documents and data forthwith" and to bar "contractors whose security clearance is not complete . . . from accessing confidential trust information, pending completion of the Master's investigation" at which time "permanent relief can be fashioned by the Master and this Court." Id. at 10.

[2] The Motion for Emergency TRO represents plaintiffs' second filing regarding OIRM. On March 30, 2001, plaintiffs filed a Motion for Special Master to Investigate The Office of Information Resource Management For Failing To Implement Adequate Security Measures and the Interior Secretary And Her Employees' And Counsel's Related Representations and Recommend Immediate And Long-Term Corrective Action and Disciplinary Measures, as Appropriate, ("Motion to Investigate"). There, plaintiffs ask the Special Master to: (a) "investigate the failure of the Interior Secretary to implement adequate security measures at OIRM to ensure that all electronic and hard copy IIM-related trust documents and data are protected fully; (b) assess the impact of such failure; (c) assess the veracity . . . regarding the security of OIRM trust documents and data; (d) investigate whether [Interior] willfully attempted to obstruct the Special Master . . . (d) recommend . . . . corrective action and disciplinary measures, as appropriate." Motion to Investigate at 7. Plaintiffs' motion was filed in response to the March 12, 2001 Site Visit Report of the Special Master to The Office of Information Resource Management. In light of the findings and recommendations contained in the instant Report, plaintiffs' Motion to Investigate is denied as moot.

("CIO") Dominic Nessi observed that,

> [f]or all practical purposes, we have no security, we have no infrastructure, ... Our entire network has no firewalls on it. I don't like running a network that can be breached by a high school kid. I don't like running a program that is out of compliance with federal statutes, especially when I have no ability to put it into compliance.[3]

Katherine McIntire Peters, *Trail of Troubles,* Government Executive, April 1, 2001 at 100.[4]

At the request of the Court, the Special Master launched an investigation into the trust data security systems in the custody or control of the Department of the Interior ("Interior" or "DOI").[5] Toward that end, the Special Master interviewed government employees and private contractors, reviewed relevant statutes and regulations, evaluated reports generated by public agencies and private

---

[3] This was not the first time that Nessi publicly questioned the integrity of BIA's IT Security. In a September 11, 2000 article published in Government Computer News, Nessi – only recently appointed to the position of Chief Information Officer Nessi – remarked that BIA is behind the times and is only now addressing the issues many agencies began work on in the mid and late 1990s insofar as the "top managers wouldn't even know what systems are in existence;" and that "[t]here really is no mentality of security. . . . People trade passwords back and forth. There wasn't proper management for removing people's access to systems after they left. There were no security background checks conducted at all." Nessi further lamented that "[t]he Bureau of Indian Affairs has no idea what it spends on IT," explaining that "[w]e can't expect the Office of Management and Budget or Congress to appropriate funds for a function if an agency doesn't plan properly or document its needs to show how it is going to utilize its funds." Tony Lee Orr, Government Computer News, *BIA Suffers High-Tech Growing Pains,* (Sept. 11, 2000).

[4] Government Executive is a monthly business magazine "serving senior executives and managers in the federal government's departments and agencies." *About Us,* <http://www.govexec.com/about.htm> (Visited Nov. 9, 2001).

[5] Although the primary thrust of this report focuses on the safeguarding of data retained on DOI/BIA/OIRM computer systems, it touches briefly on issues impacting other forms of security, namely personnel security, (i.e., "(1) defining the job, normally involving the development of a position description; (2) determining the sensitivity of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) training,"), NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook at 109, and physical security, (i.e., "measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment."). Id. at 167.

organizations and pored over thousands of pages of internal memoranda, correspondence and e-mail transmissions. The Special Master also retained the services of an independent firm with an expertise in security systems to conduct penetration tests and assist in the ultimate evaluation of the current state of Interior's Information Technology ("IT") Security.[6]

The Special Master's findings and recommendations are as follows:

II. BACKGROUND

In December 1999, the United States District Court for the District of Columbia ordered Interior to correct four breaches of statutory trust duties contained in the American Indian Trust Management Reform Act of 1994. See Cobell v. Babbitt, 91 F.Supp.2d 1,58 (D.D.C. 1999). The first two breaches implicated the agency's broad policies and procedures regarding trust accounts ("individual Indian monies" or "IIM's") while the remaining two required the Department to establish written policies and procedures for computer and business systems architecture necessary to render an accurate accounting of the IIM trust and establish written policies and procedures for the staffing of trust fund management functions necessary to render an accurate accounting of the IIM trust. Cobell, 91 F.Supp.2d at 43-45.

The Court, on that score, held that,

> [a]s impressive as Interior's new computer systems appear to be, these computer systems still depend upon the labor and skill of Interior's employees. Missing and backlogged information must be put into the computer systems. The information contained in and processed by the computer systems must be monitored and verified.

---

[6] For the purpose of this report, "information technology" will be defined as in the Clinger-Cohen Act, 40 U.S.C. § 1401(3)(A), i.e., "any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by [an] executive agency."

> Problems arising from the integration of the computer and business systems must be addressed.

Cobell, 91 F.Supp.2d at 45 (emphasis added).[7]

It is the thesis of this Report that a fundamental component of Interior's duty to monitor and verify trust information "contained in and processed by the computer systems" necessarily includes an obligation to ensure its integrity. This Report chronicles Interior's compliance with that duty in an effort to underscore the sheer enormity of the dangers to which this trust information is being exposed.

---

[7] The Court stayed its hand from awarding

> more extensive prospective relief [based] on defendants' plans (in both substance and timing) to bring themselves into compliance with their trust duties declared today and provided for explicitly by statute. These plans have been represented to the court primarily through the High Level Implementation Plan, but also through the representations made by government witnesses and government counsel.

Cobell v. Babbitt, 91 F.Supp.2d at 59.

The Circuit clarified the District Court's holding regarding the federal government's trust responsibilities when it ruled that,

> The government's broad duty to provide a complete historical accounting to IIM beneficiaries necessarily imposes substantial subsidiary duties on those government officials with responsibility for ensuring that an accounting can and will take place. In particular, it imposes obligations on those who administer the IIM trust lands and funds to, among other things, maintain and complete existing records, recover missing records where possible, and develop plans and procedures sufficient to ensure that all aspects of the accounting process are carried out. As the district court concluded, this may well include an obligation to develop or obtain computer software capable of tracking and reconciling fund data, hire staff sufficient to execute management duties, and implement specific plans to ensure that all reasonable efforts are made to provide the most complete and accurate historical accounting of IIM trust funds that is possible. The failure to implement a computer system is not itself the breach. Rather it is indicative of appellants' failure to discharge their fiduciary obligations in a reasonably prompt manner. It is the latter which constitutes the breach.

Cobell v. Norton, 240 F.3d 1081, 1105 (D.C.Cir. 2001).

The instant furor over the safety of trust data is not the first in this litigation. On November 5, 1999, BIA employees were informed that OIRM was to be moved from its headquarters in Albuquerque, New Mexico to a new facility in Reston, Virginia. See Declaration of Deborah Maddox, at ¶ 15 (March 17, 2000). Relying on the conclusions found in the Inspector General's September 24, 1999 Auditor's Report on the Bureau of Indian Affairs Consolidated Comparative Financial Statement for Fiscal Years 1998 and 1997 and the National Academy of Public Administration's Study of Management and Administration, then-Assistant Secretary for Indian Affairs Kevin Gover decided such a move would "remedy longstanding material weaknesses in the functioning of the office." Declaration of Kevin Gover at ¶ 6 (March 7, 2000), "strengthen the management and effectiveness of OIRM in the performance of its duties." Declaration of Kevin Gover at ¶ 8 (March 14, 2000), and increase BIA's emphasis on information technology." Livingston et al. v. the Department of the Interior, DE-0752-00-0237-I-2, Merit System Protection Board Hearing (August 23, 2000).[8]

BIA officials conceived a four-step process for undertaking the move. According to Nessi, who was then-OIRM Acting Director,

- there would be a transfer of knowledge between the existing OIRM staff and the contractor ISI/PRT[9] through having contractor staff work along side OIRM staff;
- the contractor would take over the operation of the data center in Albuquerque, NM on approximately March 13 and those OIRM personnel who had accepted the transfer would move to Reston, Virginia;
- the relocated OIRM staff would then begin construction and testing of the new data

[8] Page numbers are not available for the transcript of this proceeding.

[9] BIA contracted with Interior Systems, Incorporated ("ISI"), who teamed with PRT Group, Incorporated ("PRT") "to handle the IT aspects of the move." Declaration of Dominic Nessi at ¶ 15 (March 20, 2000).

center in Reston; and

- Only after the Reston facility was fully functional and ready would operations cease in Albuquerque and commence in the new Reston facility.

Declaration of Dominic Nessi at ¶ 16 (March 20, 2000). The contract between BIA and PSI/IRT provided that the contractors were to begin work at the Albuquerque facility on February 29, 2000[10] and the physical relocation was to commence during the first week of March 2000.[11]

On March 7, 2000, plaintiffs filed their Motion for a Temporary Restraining Order ("TRO") asking the court to "immediately bar all contractor access to all confidential individual Indian trust data until and unless Defendants and their attorneys demonstrate to the satisfaction of the Special Master that they are in full compliance" with a host of relevant statutes and regulations pertaining to information security. Proposed TRO at 1. Plaintiffs argued that a TRO should be imposed because OIRM contractors were "using temporary workers, who have not received proper security clearance, to review and inventory confidential IIM trust records." Motion for TRO at 2. On March 7, 2000, the Court granted plaintiffs' motion and agreed to schedule a hearing for a preliminary injunction upon review of the papers. March 7, 2000 Hearing at 43.[12]

On March 8, 2000, defendants filed a Motion for Clarification of Temporary Restraining

---

[10] See Order No. NBCWOP00371, Contract between ISI and NBC (Feb. 29, 2000).

[11] See Statement of Charles Findlay, Esq., United States Department of Justice, March 7, 2000 Hearing at 26, ("The move has already begun. It began at the beginning of this week. Employees will be leaving the Albuquerque office by the end of this week, and those who are moving to Washington, about 20 out of 60, are to report to work in Reston on Monday. Some have already begun to arrive.")

[12] The Court signed Plaintiffs' Proposed Order with the only change being that instead of the requirement to "demonstrate [compliance] to the satisfaction of the Special Master," defendants would have to demonstrate compliance to the satisfaction of the Court.

Order, requesting that the scope of the TRO be limited in its application to the ISI/PRT contractors. Defendants argued that, to bar all contractor access to OIRM "would force the Office to discontinue services" (Motion for Clarification of TRO at 2) because "[w]ithout their support, the Office would be nearly inoperable." Id. at 3. Plaintiffs opposed this motion, arguing instead that all contractors who lacked proper security clearances should be barred from OIRM. See Plaintiffs' Opposition to Defendants' Motion for Modification of TRO at 1. On March 16, 2001, the Court granted defendants' motion.

On April 4, 2000, the Court dissolved the TRO and denied plaintiffs' request for preliminary injunction on the grounds that, acting otherwise risked "harming the very beneficiaries of these trust records who will have critical payments delayed by the disruption of operations that would occur if the preliminary injunction issued," April 4, 2000 Hearing at 12.

III. SYSTEMS HOUSING TRUST DATA

Individual Indian trust information is housed on a number of computer systems and platforms throughout the country. Primary responsibility for maintaining and designing these systems rests with the Office of Information Resources Management ("OIRM") the office charged with the administration of the BIA's "computer systems and the information systems serving Indian Affairs programs such as Social Services, Law Enforcement and some components of the Trust Services systems." Decl. of former Assistant Secretary for Indian Affairs Kevin Gover at ¶ 2 (March 14, 2000).

OIRM's trust-related responsibilities include maintaining the Land Records Information Systems ("LRIS") and the Integrated Records Management System ("IRMS") – together referred to as the "legacy systems." Id. at ¶ 3. The LRIS system has been in continuous operation since 1980 (see

LRIS System Security Plan (June 30, 2001) at 5)[13] and is used by BIA Land Titles and Records Offices to "(1) provid[e] full land title service to the administrators and owners of Indian lands and to such other entities as may be authorized by law; and (2) maintain and record title, current and historical ownership of Indian land owners." Id. at 6. It's functions are housed on an IBM XXXXXXXXXXXXXXXXX mainframe located in Denver, Colorado. Id. at 8. LRIS "is the official record of all lands with which the BIA trust system deals." Id. at 7. It serves as "the accounting basis on which large sums of money are received from non-Indians and paid out to Indians." Id.

The IRMS, operational since 1982, "receives information keyed in by IRMS users at Regional Offices, Agencies, and Tribes, as well as files that are uploaded from other BIA systems. The information is used for tracking individuals, leases, and ownership and to calculate and distribute payments in the form of checks or direct deposits to thousands of Indian bank accounts." IRMS System Security Plan (June 30, 2001) at 7.

IRMS consists of six databases – five of which are operated by the Office of Trust Responsibility. IRMS System Security Plan at 6. The five Office of Trust Responsibility databases include the Lease/Range and Lease Distribution databases – which manage payouts for leases of Indian land; the Ownership database – which tracks titles of Indian tribal and trust land; the Individual Indian Monies database – which tracks funds to individual Indians from leases, royalties, permits and other uses of Indian land; and the Oil and Gas database, which manages payouts for leases of Indian owned

[13] A "System Security Plan" is designed to: "(1) provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; and (2) delineate responsibilities and expected behavior of all individuals who access the system." NIST Special Publication 800-18, Guide to Developing Security Plans for IT Systems, (Dec. 1998) at 2. All 5 system security plans cited in this report were drafted by SeNet.

Oil and Gas producing assets. Id. at 7.[14] IRMS functions are run on a Unisys NX platform located at the BIA's Reston Data Center. IRMS System Security Plan at 6.

Trust data is also housed in the Trust Asset and Accounting Management System ("TAAMS") which runs on an AS/400 platform located in Addison, Texas. See TAAMS System Security Plan, June 30, 2001 at 7. The TAAMS System is operated by Applied Terravision Systems, Inc. ("ATS"), id. at 4, which "owns, operates, and maintains the [Addison, Texas] data center's AS/400 computer." Physical Security Implementation Guidelines TAAMS Data Center, Addison, TX (June 16, 2000) at 3. As of June 30, 2001, TAAMS was touted to be the "system of record" for the Muskogee, Billings, Alaska and Anadarko offices. Id. at 5.[15]

When fully implemented, TAAMS is projected to:

> manage 56 million acres of trust land, 170,000 tracts of land, 100,000 active land leases, 350,000 owners of land parcels, and 2 million owner interests. The system will serve 3,000 users, with an estimated 1,500 users logging in daily and accessing records concurrently. TAAMS is replacing a number of existing legacy systems such as LRIS, IRMS and RDRS. Unlike these batch-based legacy systems, TAAMS is based on modern database, client/server, and networking technologies, that considerably improve performance, efficiency and reliability.

TAAMS Systems Security Plan at 6.

The systems containing trust data are linked by the BIA Wide Area Network[16] ("BIANET")

---

[14] The sixth IRMS database is owned by the Office of Tribal Services. IRMS System Security Plan at 6.

[15] According to Deputy Director of the BIA Office of Economic Development George Gover, the term "system of record" is "a term of records management. . . . That is the system you stand by. That is the official system, official position of what the record should look like." August 14, 2001 Interview of George Gover at 36-37.

[16] A wide area network (WAN) "is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A

that connects over 5000 users in sites nationwide to centralized BIA and DOI computing resources and services. By using the BIANET, “ users in the 48 CONUS states and Alaska can access, retrieve, and manipulate information residing on BIA and DOI computing resources, exchange e-mail messages with DOI employees, use the Internet to exchange e-mail with individuals in other government and commercial organizations, and browse the Internet for general information.” BIANET System

---

wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.” <http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci213336,00.html0o>

Security Plan (June 30, 2001) at 7. The information transmitted therein "ranges from public domain to highly sensitive." Id.

Another system linking computers which house trust data is the Reston, Virginia Local Area Network ("Reston LAN")[17] that provides users in the Reston Office access to IT resources, e.g., mail servers, printing, Internet access, and provides nationwide users with access to BIA major applications that are hosted on computer system inside the Reston data center.[18] Transmitted information ranges from non-sensitive to highly sensitive. Reston LAN System Security Plan, (June 30, 2001) at 7-8.

IV. DUTY TO SAFEGUARD TRUST INFORMATION

In the normal course of business, Interior retains a wide range of trust data relating to the plaintiff class of individual Indian account holders and beneficiaries. This data constitutes inherently sensitive business information which must be stored and handled in a secure environment that has been

---

[17] A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network). <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212495,00.html>

[18] IRMS is considered BIA's "major application" housed at the Reston facility. IRMS System Security Plan at 6.

adequately safeguarded from intrusion, alteration or destruction by unauthorized parties. See BIA IT Risk Assessment (January 4, 2000) at 4 ("both because of the distributed nature of its IT resources and user population as well as the sensitive information it maintains on tribes and individual Indians. . . . [t]his information must, by law, be protected from unauthorized access, alteration or destruction."). The duty to protect this sensitive information may be traced to several sources.

A. **Common Law**

Interior's substantial trust responsibilities toward Native Americans, including the responsibility to safeguard records, is "undeniable" and grounded "in the very nature of the government-Indian relationship," Cobell v. Norton, 240 F.3d 1081, 1085 (D.C.Cir. 2001) (citing United States v. Mitchell, 463 U.S. 206, 225 (1983)), and in well established common-law fiduciary principles. See Security & Exchange Comm. v. Sargent, 229 F.3d 68, 76 (1st Cir. 2000) (recognizing "fiduciary duty to safeguard information relating to" trust); Rippey v. Denver U. S. Nat. Bank, 273 F.Supp. 718, 735 (D.C.Colo. 1967) ("It is generally agreed that a trustee owes a duty to his beneficiaries to exercise such care and skill as a man of ordinary prudence would exercise in safeguarding and preserving his own property."); Rest. 2d Trusts § 173 (Comment C)(trustee should preserve records in a manner that provides trust beneficiaries access "to such information as is reasonably necessary to enable [them] to enforce [their] rights under the trusts or to prevent or redress a breach of trust.").

Indeed, the duty "to furnish to the beneficiary on demand all information regarding the trust and its execution which may be useful to the beneficiary in protecting his rights" Cobell v. Babbitt, 91 F.Supp.2d 1, 42 (D.D.C. 1999) (quoting George T. Bogart, Trusts § 141 (6th ed. 1987)) would be

rendered meaningless unless the underlying information were adequately secured.[19]

B. **Statutory and Regulatory Guidelines**

In addition to the fiduciary obligations imposed by common law, defendants' responsibilities are codified in, and governed by, an exacting set of statutes and policies including:

- The Privacy Act of 1974, 5 U.S.C. § 552a, which, in relevant part, provides that, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. . . ;"

- The Freedom of Information Act of 1974, 5 U.S.C. § 552, which requires agencies to "make reasonable efforts to search for [requested] records in electronic form or format. . . ;"

- The Paperwork Reduction Act of 1978, 44 U.S.C. § 3501, which attempts to make "uniform federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of government programs;"

- The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701, which criminalizes unauthorized access to electronic communications;

- The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, which criminalizes unauthorized access to information stored on government computer systems;

- The Computer Security Act of 1987, 40 U.S.C. §1441(amended by the Clinger-Cohen Act), which requires the government to promulgate standards for computer security, train relevant employees in computer security and establish plans for the security and privacy of computer information. In relevant part, the Act requires that "each federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of each Federal computer system within or under the supervision of that agency," and "establish a plan for the security and privacy of each Federal computer system . . . that is commensurate with the risk

---

[19] On that score, this jurisdiction has spoken with a clear voice when it held that "[c]ourts 'must infer that Congress intended to impose on trustees traditional fiduciary duties unless Congress has unequivocally expressed an intent to the contrary.'" Cobell v. Norton, 240 F.3d 1081, 1099 (D.C.Cir. 2001)(quoting NLRB v. Amax Coal Co., 453 U.S. 322, 329 (1981)).

and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system;"

- The Clinger-Cohen Act, 40 U.S.C. § 1401 (formerly known as the Information Technology Management Reform Act), which directs executive agencies to establish the position of Chief Information Officers and places responsibility for "providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency . . .; developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency" on the CIO;

- The Trade Secrets Act, 18 U.S.C. § 1905, which criminalizes unauthorized government disclosure of trade secrets;[20] and

- The Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. § 2512, which directs executive agencies to file reports detailing whether "the accounting system of the agency conforms to the principles, standards, and requirements the Comptroller General prescribes."

C. **Executive Branch Guidelines**

Interior's common-law responsibilities and their statutory counterparts have been underscored in Executive Guidelines and Procedures, including,

- The Office of Management and Budget Circular A-130, Management of Federal Information Resources, (Nov. 28, 2000) and Appendix III to Circular A-130,which establishes policies for the management of Federal information resources. Circular A-130 directs agencies to "plan in an integrated manner for managing information throughout its life cycle" and requires that agencies "[e]nsure that information is

[20] Although the term "trade secrets" is not defined in this statute, courts have generally borrowed the definition from the Uniform Trade Secrets Act to include information that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public," provided that "the owner thereof has taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3) (Supp. 1997); see also D.C. Code Ann. § 48-501(4) (1997) (paraphrased definition).

protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information," and that agencies "must make security's role explicit in information technology investments and capital programming." The Circular also sets out specific guidelines for agencies to ensure the security of information systems;

- The Office of Management and Budget Circular A-123, Management Accountability and Control, (June 21, 1995), which "provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls";

- The Office of Management and Budget Circular A-127, Financial Management Systems, (July 23, 1993),which "prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems";

- OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information (July 9, 1990), whose purpose "is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. This Bulletin supersedes OMB Bulletin No. 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information" (July 6, 1988)";

- February 28, 2000 Memorandum for the Heads of Departments and Agencies from Office of Management and Budget Director Jacob Lew, which directs agencies to plan for IT Security needs, by making "security's role explicit in information technology investments and capital programming";

- National Security Telecommunications and Information Systems Security Committee Publication 1000, National Information Assurance Certification and Accreditation Process (April 2000), which "establishes a standard national process, set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site."

D. **Industry Standards**

Finally, executive agencies, such as Interior are directed by guidelines promulgated by the National Institute of Standards and Technology ("NIST")[21] and the Federal Information Processing

[21] NIST "works with industry, research, and government organizations to make [information] technology more usable, more secure, more scalable, and more interoperable than it is today." Dr. William O. Mehuron, *Information Technology Laboratory: What ITL Does*<http://www.itl.nist.gov/itl-what_itl_does.html> (Last Modified Nov. 15, 2000).

Standards ("FIPS").[22] These include:

- NIST Special Publication 800-10, Keeping Your Site Comfortably Secure: an Introduction to Internet Firewalls (Feb. 1995), which "provide[s] a basis of understanding of how firewalls work and the steps necessary for implementing firewalls." Id. at ix;

- NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems (Sept. 1996) which "provides a baseline that organizations can use to establish and review their IT security programs." Id. at 1. In the most recent version of the Information Technology Security Program covering OIRM activities, the Department of the Interior acknowledges that "NIST SP 800-14 provides the foundation for meeting the minimum requirements for the protection of Federal IT systems and hosted data." The Office of the Assistant Secretary Indian Affairs Information Technology Security Program Version 1.1, May 17, 2001 at 4;

- NIST Special Publication 800-12, Introduction to Computer Security: the NIST Handbook (Oct. 1995) which "provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations." Id. at 3;

- NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role and Performance Based Model (April 1998), which provides a framework for IT Security Training that is both "appropriate for today's distributed computing environment and [flexible] for extension to accommodate future technologies and the risk management decisions." Id. at 4;

- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (Dec. 1998), which "show[s] what should be done to enhance or measure an existing computer security program or to aid in the development of a new program." Id. at 2;

- NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (June 2001), which presents "a list of system-level security principles to be considered in the design, development, and operation of an information system." Id. at 1;

---

[22] Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. *General Information*, <http://www.itl.nist.gov/fipspubs/geninfo.htm> (Last Modified Aug. 30, 2001).

- NIST Special Publication 800-31, Intrusion Detection Systems (Aug. 2001), which is a "primer in intrusion detection, developed for those who need to understand what security goals intrusion detection mechanisms serve, how to select and configure intrusion detection systems for their specific systems and network environments, how to manage the output of intrusion detection systems, and how to integrate intrusion detection functions with the rest of the organizational security infrastructure." Id. at 5;

- FIPS Publication 31, Guidelines for ADP [Automatic Data Processing] Physical Security and Risk Management (June 1974), which "provides a handbook for use by Federal organizations in structuring physical security and risk management programs for their ADP facilities." Id. at 1;

- FIPS Publication 73, Guidelines for Security of Computer Applications (June 1980), which describes "methods and techniques that can reduce the hazards associated with computer applications." Id. at 1;

- FIPS Publication 83, Guideline on User Authentication Techniques for Computer Network Access Control (Sept. 1980), which "provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks." *FIPS Publications*, <http://www.itl.nist.gov/fipspubs/by-num.htm> (Last Modified July 3, 2001);

- FIPS Publication 87, Guidelines for ADP Contingency Planning (March 1981), which "describe for organizational and data processing management, and for managers who obtain data processing services from other activities, what should be considered when developing a contingency plan for an ADP facility." Id. at 1;

- FIPS Publication 102, Guidelines for Computer Security Certification and Accreditation (Sept. 1983), which "describes how to establish and carry out a certification and accreditation program for computer security." Id. at 1;

- FIPS Publication 112, Password Usage (May 1985), which "establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used." *FIPS Publication 112*, <http://www.itl.nist.gov/fipspubs/fip112.htm#FORE_SEC> (Visited Nov. 7, 2001);

- FIPS Publication 191, Guidelines for the Analysis of Local Area Network Security (Nov. 1994), which "discusses threats and vulnerabilities and considers technical security services and security mechanisms" for Local Area Networks. *FIPS Publication 191*, <http://www.itl.nist.gov/fipspubs/fip191.htm> (Visited Nov. 7, 2001).

V. **REPORTS EVALUATING INTERIOR'S IT SECURITY PROGRAM**

To date, there have been at least 30 reports generated by both governmental and private organizations including the Office of the Inspector General ("OIG"), the General Administration Office ("GAO"), a House of Representatives Subcommittee, Arthur Andersen & Co. ("Andersen"), SeNet International ("SeNet"), the Special Master and Predictive Systems, Incorporated ("Predictive") which have addressed the state of IT Security at the DOI. A detailed review of these reports, findings, and where applicable, recommendations, is a necessary predicate to evaluating the current state of IT Security and recommending a course of action.

A. **Arthur Andersen & Co. Reports**

The first known reports generated by a private organization addressing Interior's IT Security issues were those published by the public accounting firm of Arthur Andersen & Co. The first of these reports – a Report of Independent Public Accountants – was issued on March 23, 1989 to the Bureau of Indian Affairs following an audit of the assets, liabilities and fund balances of the Public Monies of the United States managed by the BIA. On May 11, 1990, Andersen issued a second Report auditing the assets and trust fund balances of the Tribal and Individual Indian Monies Trust Funds controlled by the BIA.

1. **Arthur Andersen & Co. Reports: Findings**

Andersen found that:

Report Date	Report Title	Problem	Page
1989	Report of Independent Public Accountants	"Data processing controls throughout the Bureau cannot be relied upon to ensure that data are being properly processed. Data processing is conducted at various locations throughout the Bureau, and, at certain locations, there are inadequate controls over systems and data, inadequate segregation of duties, and deficiencies in controlling systems development."	8
		"System errors were found for which no corrective action had been taken."	50
		"The NTSC [National Technical Support Center] does not have a current disaster recovery plan."	57

		"On Saturday morning February 11, 1989, an outside auditor was able to achieve unauthorized access to the NTSC programming and management areas. The design of the door to the NTSC allowed unauthorized access outside the normal work hours to the programming and management areas. There is an alarm on the door that goes off when the door is opened by unauthorized personnel during the normal workday. However, on the above mentioned date, the alarm did not go off."	59
		"Each IMC [Information Management Center] is limited as to the number of people that can be employed. As a result, it is difficult to segregate duties between computer specialists (programmers), computer assistants and operators. During our review of the IMC's, we noted that computer specialists have the ability to access and alter master data files, application systems programs and certain operating system programs."	59
Report Date	Report Title	Problem	Page
		"The ability of the computer specialists to access and alter the master data files and the application files permits the programmers the ability to compromise the integrity of the data and data processing. A computer specialist has the ability to create a new account, transfer funds to the account and process a check. Further, alterations to IRMS programs could be made to allow the checks to be printed, but not recorded on the check register."	60
		"Discussions with computer specialists indicated that minor changes requested by users do not require IMC manager approval to be made. Unauthorized changes to the IRMS programs could be made that may reduce the integrity of the data and the processing."	61
		"Discussions with computer specialists indicated that there are no formal testing procedures. In addition, we were made aware that certain testing is performed using actual 'live' data in the production mode."	61
		"Through discussions with various personnel, we noted the operators, computer assistants and computer specialists all had access to various password files."	63
		"A periodic maintenance and inspection contract for the Halon fire control system is not in place."	65

		"The daily tape backup library is not adequately fire protected. While most tape libraries are located adjacent to the computer operations room, . . in some instances, there was not fire protection in the tape room itself."	65
1990	Report of Independent Public Accountants	"Data processing controls throughout the Bureau cannot be relied upon to ensure that data is properly processed."	9
		"Management indicated [access controls over master data files] is still a problem due to the small number of personnel and the security system available for the hardware."	26
		"Presently, the policy of changing passwords every 30 days has been implemented at the NTSC but is not fully effective at the IMCs."	26

2. **Arthur Andersen & Co. Reports: Recommendations**

The 1989 Andersen Report recommended that:

1. "a disciplined controllership function [be imposed]: Summary reports of activity and cumulative balances of the Trust Funds . . . be reviewed by management personnel who are familiar with financial reports and generally accepted accounting principles, as they apply to the Trust Funds; Procedures and controls must be developed and then followed to ensure that accounting entries which impact the Trust Funds are properly reviewed. These procedures and controls must be adequate to ensure that all activities at Area and Agency Offices are properly reviewed; The various accounting systems and subledgers used by the Bureau must be reconciled to each other and discrepancies must be resolved. [T]he systems currently being used must be reconciled to ensure the integrity of information currently being processed by the Bureau." Arthur Andersen & Co. Report of Independent Public Accountants (March 23, 1989) at vii.

2. "an audit process [be implemented] to verify that controls and procedures are functioning effectively and that recorded balances are accurate: a. An internal audit function should be established to provide an ongoing review of compliance with controls, procedures and regulations. The internal audit group should communicate with upper management or an oversight group to maintain independence from operations and accounting personnel; b. An annual audit by independent public accountants should continue to be performed. The independent annual audit provides an objective view of the organization, its controls and procedures and financial accounting policies." Id. at vii.

3. "Area Offices reflect each Agency Office's results of operations should be analyzed on

a monthly basis for trends and unusual fluctuations and reconciled to other sources, as appropriate." Id. at 30.

4. "accounts be established in the general ledger and IRMS systems to track receipts and disbursements activity, similar to the general ledger accounts established for the Tribal Trust Fund." Id. at 30.

5. "in order to ensure a more accurate balance in both IRMS and the Finance System, system errors should be promptly corrected when these errors are discovered." Id. at 50.

6. "a computer programming change be made to reflect proper cut-off on the account statements." Id. at 50-51.

7. "the CV [collection voucher] number log and official report file be reviewed weekly so that such errors can be caught and corrected. On a Bureau-wide level, CV's should be prenumbered and issued by the Central Office-West, and control should be maintained at the Area Office level. This would provide uniformity throughout the Bureau, and more centralized control." Id. at 51.

8. "all Agency Offices implement the IRMS system and train employees on the use of the system." Id. at 52.

9. "the Bureau . . . consider providing teams that assist with the implementation and training of IRMS capabilities." Id. at 52.

10. "upon notification of death, the management code be appropriately changed." Id. at 53.

11. training be provided to IIM clerks "in the various account codes and their meaning." Id. at 53.

12. "the Agency Superintendent assure that all name, address and management code changes were input properly by reviewing a summary of changes report." Id. at 53.

13. "NISC develop and test a workable disaster recovery plan. The disaster recovery plan developed should, at a minimum, address the following issues: Levels of response to several possible disasters; Hardware requirements; Remote processing requirements Telecommunications requirements; Data-entry support; Operating system support; Other systems software; Application systems software; Data file storage and retention; Forms; System operation procedures; User procedures; Staff responsibilities; Plan maintenance." Id. at 57-58.

14. "NTSC consider establishing a full-time ADP internal audit function to help ensure that

ADP internal controls are in place and operating effectively. The internal auditor should report to a high level of management that has no routine ADP responsibilities but has authority over NTSC and has a good understanding of ADP operations." Id. at 58

15. "NTSC management implement a procedure to verify that the above mentioned door alarm is operating effectively outside of the normal work hours or provide another means of security to prevent access." Id. at 59.

16. "master data files be password protected. The control of the master data passwords should be placed in the hands of the data owner or a security officer. If access to master data files by IMC personnel is required, the access should be requested from the data owner, i.e., user. In addition, computer specialists should be given access only to test versions of the application programs. The production version should be controlled by password. Access to the production version should be given to the IMC manager, who should have the responsibility of transferring programs to the test area, and back to production after modification, testing and review procedures have been performed. This segregation of duties could be accomplished by placing access passwords on different user packs." Id. at 59-60.

17. "in conjunction with [the] recommendation on the segregation of duties, the IMC manager review and approve all modifications prior to transferring the modified programs back to production." Id. at 60-61.

18. "[a]ll modifications made to programs or data files . . . be approved by the IMC manager prior to being made and then reviewed by the manager after being made and prior to placing them into production." Id. at 61.

19. "a test environment be defined for each system, and that formal testing procedures be put in place. The procedures should be tailored to include small as well as large modifications. At a minimum, testing should be performed in a section of the computer not related to the production section. Formal testing procedures allow a structure for adequate and consistent testing. Testing procedures should include the following: Test all known combinations including realistic volume estimates; Test using user prepared test data; Perform complete and comprehensive testing prior to moving the application into production; Test all interfacing systems to evaluate the integrity of the interface; Develop conversion procedures to assure proper cutoffs and conversion of data files; Test user procedures and other manual procedures; Perform tests only on test files; Establish a standard naming convention for all test programs; Have user and ADP management approve the test results prior to conversion to a new application system." Id. at 61-62.

20. "even more emphasis be placed on ensuring the users are involved in all phases of application modifications, i.e., planning, implementation and testing." Id. at 62-63.

21. "a policy be developed which requires a periodic change of the user passwords. We further recommend the users be instructed to request a password change whenever they believe their password has been compromised." Id. at 63.

22. "the password files be protected to allow only designated personnel to access and modify these passwords. We further recommend the application passwords be controlled by the user departments." Id. at 63-64.

23. "[t]he disaster recovery plan . . . be tested. All phases of the plan, including offsite processing, should be made part of the test. The test should be rehearsed and controlled to maximize the learning value of the employees." Id. at 64.

24. "each IMC obtain a contract that would require a periodic maintenance and evaluation of the Halon system by a qualified contractor." Id. at 65.

25. "fire protection be added to the tape libraries for both on- and off-site storage areas. This protection should include a separate Halon nossle [sic] and fire rated walls, floors and ceilings." Id. at 65.

B. **Office of the Inspector General Reports**

Reports issued by the Department of the Interior's OIG represent the first reports published by the government exposing Interior's IT security deficiencies. Of those made available to the Special Master, nine provided information pertinent to trust data. Those reports analyzed:

1. Whether the Bureau of Indian Affairs National Irrigation Billing System "(1) had been adequately planned by the Bureau, (2) fulfilled the interface requirements of centralized accounting for the Bureau, (3) had effective controls, and (4) could be used to bill for all irrigation projects regardless of billing components." OIG Report No. 94-I-688: National Irrigation Billing System, Bureau of Indian Affairs at 1 (June 1994);

2. "[T]he Statement of Assets and Trust Fund Balances for the Tribal, Individual Indian Monies and Other Special Appropriation Funds managed by the U.S. Department of the Interior Bureau of Indian Affairs Office of Trust Funds Management ('OTFM') as of September 30, 1995." OIG Report No. 97-I-196: U.S. Department of the Interior Bureau of Indian Affairs Tribal, Individual Indian Monies and Other Special Appropriation Funds Managed by the Office of Trust Funds Management at 1 (September 30, 1995);

3. The general controls at the Operations Service Center including "controls for security program development, access, software development and change control, segregation of duties, system software, and service continuity as they relate[] to the two mainframe computers and to Center operations." OIG Report No. 97-I-771: General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs at 2 (April 1997);

4. The Mineral Management Service's "six major areas: security program development;

logical and physical access; software development and change management; separation of duties; system software; and service continuity." OIG Report No. 98-I-336: General Controls Over the Automated Information System, Royalty Management Program, Mineral Management Service at 3 (March 1998);

5. "[T]he actions taken by Bureau management to implement the 13 recommendations made in [the] April 1997 audit report." OIG Report No. 98-I-483: Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs at 2 (June 1998);

6. The "actions taken by Bureau management to implement the 12 recommendations contained in [the] April 1997 audit report and the 8 recommendations contained in [the] June 1998 audit report and a review of the general controls in place during fiscal year 1998." OIG Report No. 99-I-454: Followup of Recommendations for Improving General Controls Over Automated Information Systems, Bureau of Indian Affairs at 2 (July 1999);

7. "[T]he statements of assets and Trust Funds balances and the statements of changes in Trust Funds balances for Tribal and Other Special Trust Funds and for Individual Indian Monies Trust Funds as of and for the fiscal years ended September 30, 1998, and 1997." OIG Report No. 00-I-434: Independent Auditors Report on the Financial Statements for Fiscal Years 1998 and 1997 for the Office of the Special Trustee for American Indians Tribal and Other Special Trust Funds and Individual Indian Monies Trust Funds Managed by the Office of Trust Funds Management at 5 (May 2000);

8. "[T]he financial statements of the Office of the Special Trustee for American Indians." OIG Report No. 01-I-205: Independent Auditors Report on the Financial Statements for Fiscal Years 1999 and 1998 for the Office of the Special Trustee for American Indians Tribal and Other Special Trust Funds and Individual Indian Monied Trust Funds Managed by the Office of Trust Funds Managements at 2 (January 2001);

9. "[T]he Bureau of Indian Affairs' (BIA) principal financial statements for the fiscal year ended September 30, 2000." OIG Report No. 01-I-385: Independent Auditors Report on the Bureau of Indian Affairs Financial Statements for Fiscal Year 2000 at 2 (May 11, 2001).

1. **Office of the Inspector General: Findings**

Concerns about IT Security at the BIA first surfaced in the June 1994 audit report generated by the OIG.[23] That report, and others that followed, exposed shortcomings relative to breaches in

[23] While the OIG Final Audit Report to the BIA generated on September 27, 1988 references an "ongoing review of automated data processing activities within the Bureau of Indian Affairs," specific

physical security, personnel security and data security:

Report Date	Report Title	Problem	Page
June 1994	Survey Report: National Irrigation Billing System, Bureau of Indian Affairs	"Access to the National Irrigation Billing System was not adequately controlled to ensure the accuracy and validity of critical accounting and financial data maintained in the System. Management officials and software programmers could add, change, and delete without sufficient audit trails to identify the individuals who entered or changed the data."	4
		"Edits did not exist in the System to prevent collections for operation and maintenance fees from being improperly posted to the construction repayment account. Since construction repayments are to be deposited in the U.S. Treasury rather than to irrigation operation and maintenance accounts, the potential exists for the Bureau to not detect the error and to lose the use of operating money."	4
		"The System did not track data entry errors that the System rejected. As a result, there was no assurance that the error was corrected and that all information was entered."	5
		"The records identifying the heirs of the original trust allotments remain inaccurate. Thus the project staff (1) manually prepare bills for the multiple heirs; (2) forward the bills to agency realty offices for debt collection, a procedure that has not been effective; or (3) do not send bills."	6
September 1995	U.S. Department of the Interior Bureau of Indian Affairs Tribal, Individual Indian Monies and Other Special Appropriation Funds Managed by the Office of Trust Funds Management	"Disaster recovery planning over the Omni application is adequate. However, our review noted there currently is no formal agreement for disaster recovery pertaining to the Unisys A-17 or the IBM 3090. Our observations also noted that the physical location of the two mainframes is at the Albuquerque Federal Court Building, a high risk location. Informal arrangements have been made with other governmental agencies to provide recovery services in the event of a disaster."	37

mention of IT security did not surface until the 1994 Report.

		"Security controls over the Unisys A-17 mainframe are inadequate. The system does not require automatic password changes periodically, users are not automatically logged out after a specified period of inactivity, and there is no limit to the number of invalid password attempts made by a user. Furthermore, our discussion noted that 'Help Desk' personnel have the ability to reinstate or reset passwords which have been revoked."	38
Report Date	Report Title	Problem	Page
		"Our review noted that changes to the Individual Indian Monies (IIM) application are not performed in a test environment on the Unisys A-17 mainframe. There are also no procedures in place for subsequent review after changes have been implemented by the programmer. Review is limited to verification of the output by the requesting party."	38
April 1997	Audit Report: General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs	"Although users were provided written information about system security issues when access to computer systems and application was approved, the Center did not have an employee computer security awareness training plan in effect. Further, the security staff had not provided periodic computer security training to Bureau area and agency offices and other organizations, such as schools."	8
		"Risk assessments had not been performed periodically or had not been performed when systems, facilities, or other conditions changed. Specifically, since 1990, only two risk assessments had been performed . . . . While we determined that these assessments were adequate, we also determined that the Center had not implemented recommendations from the risk assessments."	8
		"Assessments of the system security programs effectiveness were not performed periodically. Also, the system security program was not reviewed under the Financial Managers' Financial Integrity Act annual review process."	8
		"Major systems and applications were not always accredited by the managers whose missions they supported."	9
		"Personnel in sensitive or critical ADP positions, such as system programmers and application programmers (including application programmers not assigned to the Center), did not have documented background investigations for security clearances or did not have security clearances at a level commensurate with their positions."	11

		"Although the IBM computer had been set to automatically revoke a user identification (ID) after 180 days of inactivity, supervisors did not notify the application owner or manager or the Center's security staff to revoke and delete a user ID when an employee's employment was terminated or an employee was transferred."	11
		"The Bureau had not classified its computer resources to determine the level of security that should be provided by the Center."	13
Report Date	Report Title	Problem	Page
		"The Center was located within a Federal building (which also houses U.S. Courts) that allows unauthorized individuals access to the Center. To ensure that the Center and its resources were safeguarded, physical access to the Center was achieved by electronic keycards, and access into the Center was monitored by video cameras. However, visitors, such as custodial (contractor) personnel and building managers, had been provided the keycards and therefore had unmonitored access while in the Center."	14
		"General housekeeping and maintenance of the computer operations room were performed only weekly. This weekly schedule was inadequate because of the failure to remove potential fire hazards caused by combustible supplies and by dust produced by paper used in the printer, which was also housed in the computer operations room."	14
		"Security staff and application owners did not periodically review user access authorizations to ensure that users' levels of access to the mainframe computers were appropriate."	16
		"Passwords were not changed periodically, and inactive user Ids were not automatically revoked on the UNISYS computer. Additionally, greater reliance had to be placed on the user ID and password controls to protect the application, files, and data because the applications residing on the UNISYS computer were developed without access controls and could not be modified to install the access controls."	17

		"The software development and change control was inadequate to ensure that the proper version of an application was used in production. Based on our test of the National Irrigation Information Management System, which was managed by the Bureau's Irrigation and Power Liaison Section, we found that the application programmers not only programmed the application but also tested, authorized, and approved the movement of the modified programs from test or development into production. In addition, the lead programmer was not made aware of software modifications. Further, one member of the Center's systems staff could also move application software changes from test or development into production without the lead programmer's approval."	18
Report Date	Report Title	Problem	Page
		"Periodic reviews of the System Maintenance Facility logs and RACF[24] access reports were not performed by the security staff to monitor system activities. Additionally, the security staff produced reports that identified users and the computer resources accessed; however, the staff had not produced or used the primary 'auditing' or monitoring reports that could be used in monitoring system activities."	21
		"One system programmer had 'alter' access to system software, the System Maintenance Facility logs, and RACF logs. With this access, the programmer could alter the logging of his activities, as well as any other user activities. Thus the audit trails of system activities could be impaired or destroyed."	21

[24] RACF ("Resource Access Control Facility") reports are reviewed as a form of system auditing. See OIG Report No. 97-I-771 at 5.

		"RACF can be used to establish controls and monitor access to the computer resources. However, RACF had not been set up to effectively control access to the system resources. We found that one of the 'start procedures' had been assigned the PRIVILEGED attribute. With this attribute, the started task can bypass all verification processing, including the security classification checks, and therefore affect the overall security of the system. Additionally, with the PRIVILEGED attribute, no logging or audit trail of this task was available. Further, no datasets, including the system parameter library, linklist libraries, master catalog, and the primary and backup files, were protected by RACF."	21
		"The Center did not have an effective means to recover or to resume computer operations in the event of a system failure or a disaster. Although the Center has begun developing a service continuity plan for fiscal year 1997, the Center did not have a service continuity plan in place. Additionally, the off-site storage facility was not located at least 1 mile from the Center, and the facility did not adequately safeguard information and data stored from unauthorized access and environmental hazards such as heat or humidity."	23
March 1998	Audit Report: General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service	Program management did not "[i]dentify and address the impact that (1) converting to the year 2000 would have on application processing, (2) using system security software which is no longer supported by the vendor could have on operations, and (3) having royalty and financial information on local area network applications and personal computer databases could have on operations."	9
Report Date	Report Title	Problem	Page
		Program management did not "Correctly assess the risk for the 'Geopolitical' and 'External Directives' elements, which were assessed as low risk. Significant geopolitical and external directives, such as the possible abolishment of the Program and the enactment of the Federal Oil and Gas Royalty Simplification and Fairness Act, have impacted the Program during the past 2 years. We believe that the level of risk associated with these elements was such that it increased the potential for lowering employee morale and thus increased the risk of sabotage or breach of other physical security measures, as well as the possibility of data errors and omissions that affect data and system integrity."	9
		"Contractor employees received the same type of background check and security clearance regardless of their duties and the risk associated with the computer-related work they performed. Thus, contractor employees, such as system programmers and computer operators, who could bypass technical and operational controls, received the same security clearance as administrative assistants."	13

		"Computer-related work was not technically reviewed by contractor or Program personnel whose position sensitivity was greater than that of the position sensitivity of individuals performing the work."	13
		"Contractor employees did not always submit requests for background checks for security clearances. Further, the requests that were submitted for background checks were not submitted within the time frames specified in the contract. An average of 175 calendar days elapsed, instead of the 2 weeks stipulated in the contract, between the dates the employees were hired and the dates the requests were received by the Minerals Management Service's Security Officer in Personnel for forwarding to the Office of Personnel Management. The Office of Personnel Management performed background checks for the same employees in an average of 84 days, and the Mineral Management Service approved the security clearances in an average of 22 days. Thus, most of the delay in the security clearance process was attributable to contractor and Program personnel."	13
		"System Management Division employees did not have documentation to support that appropriate background checks for security clearances and required periodic followup background checks had been performed."	13
Report Date	Report Title	Problem	Page
		"We found that automated information system users did not have security awareness statements on file acknowledging the employees' acceptance of their responsibilities to safeguard the Program's proprietary data and assets."	17
		"The Program's computer resources (data files, application programs, and computer-related facilities and equipment) were not classified appropriately to determine the levels of access controls that should be implemented over the resources. For example, no 'major application' was identified in the Program's annual security plan, even though the applications and data files were 'proprietary' and critical to the Program in accomplishing its mission and reporting financial information. Further, access controls over sensitive data on the servers used by the Program's divisions were not as stringent as the access controls over sensitive data on the mainframe."	19

		"Default settings provided with commercial off-the-shelf software were not removed after the software was installed and implemented. For example, we found that the default user identification (ID) and associated default password had not been removed when Program management upgraded to the latest version of the Integrated Data Management System (IDMS). The default user ID provides users with administrative privileges to establish and remove users and to access all mainframe computer resources."	22
		"Resource Access Control Facility (RACF) provides the capability to set rules for passwords in which the installation can require the use of specific characters (a mix of letters and numbers) within the passwords, but this feature was not used."	24
		"A default security setting was found on a server file that allows passwords to be unencrypted."	24
		"The 'SECURE CONSOLE' command was not found on a server file which removes the Disk Operating System (DOS) from the server memory. The removal of DOS from the server memory prevents an individual from inserting a diskette into the server drive and loading unauthorized software that could perform such functions as change passwords, establish trustee rights, creates users, and assign security levels. Also, the 'SECURE CONSOLE' command disables the users' ability to change the server date and time, thus allowing users to bypass access restrictions."	24
Report Date	Report Title	Problem	Page
		"We found that controls were not adequate to ensure that access levels granted to users of the Program's automated information system were appropriate. Specifically, access managers had not approved all automated information system access granted to users of the access managers' applications and had not performed periodic reviews to determine who the users were and whether the levels of access granted in the automated information system were the access levels approved."	26
		"The Program's number of unsuccessful log-in attempts to access its automated information system exceeded the standard establish by the Department. Specifically, in 1992, Program management increased the number of unsuccessful log-in attempts from three to five before a user's ID and password were revoked."	29

		"Change management controls over client/server application software were not adequate. Specifically, we found that there were no controls to ensure that: (1) Program management authorized and approved software changes and (2) the changes to the application software were adequately tested before the changed software was moved into production."	30
		"Application programmers were authorized to access client/server production data to perform 'ongoing maintenance' on applications."	32
		"At least one application programmer acted as a backup to an end user, which required the programmer to change production data in the Minerals Management Service Appeals Tracking System."	32
		"The individual responsible for setting up users of the Royalty Management Program Desktop applications was also the person designated ro review server security logs, which record the activities of the users of the applications."	32
		"The version of RACF, the commercial mainframe security software, that was used by the Program was no longer supported by the vendor. Although the upgraded version of RACF had been purchased, it had not been implemented."	35
Report Date	Report Title	Problem	Page
		"System integrity verification and audit software was not used. This software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures such as setting system options inappropriately, installing 'back doors' to the operating system, and introducing viruses and Trojan horses, that can destroy production dependability and circumvent existing security measures."	37
		"Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. Additionally, system options that produce a system audit trail were not implemented. Therefore, an audit trail that logs the results of actions taken by computer operators and system programmers in the SYSLOG during system initialization could not be produced for periodic review."	37

		"Periodic reviews of System Management Facility (SMF) logs to identify critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records events such as 'SET TIME,' 'SET DATE,' and 'SET SMF,' all of which affect system processing and production of audit trails."	37
		"Periodic reviews of SMF logs to identify unauthorized changes to data by authorized users were not performed. Even though one of the SMF record types, record type 60, which logs all activity affecting Virtual Storage Access Method data sets that contain lease and site security data, was activated during our audit, the logs were not reviewed to detect inappropriate actions or unusual activity by authorized users."	37
		"Local area networks and personal computers used by the Program's divisions that maintain proprietary and financial data were not included in the Program's disaster recovery plans."	40
Report Date	Report Title	Problem	Page
May 2000	Audit Report: Independent Auditors Report on the Financial Statements for Fiscal Years 1998 and 1997 for the Office of the Special Trustee for American Indians Tribal and Other Special Trust Funds and Individual Indian Monies Trusts Funds Managed by the Office of Trust Funds Management	"Periodic reviews of system reports were not being performed."	55

		"Specific, clearly defined information security policies and process systems security monitoring do not exist."	55
		"As part of our audit related to [Electronic Data Processing], we reviewed physical access to the computer room, which houses the IRMS system and other critical Trust Systems equipment and documents. At the present there are 103 active access cards. Based upon our review we noted not all cards are assigned to specific individuals; certain individuals are in possession of multiple cards; a number of contractors with limited need are in possession of access cards; a number of OSC personnel whose job function should not require access to the computer room are in possession of access cards; two individuals from the Division of Accounting Management are in possession of access cards. Control measures to protect Trust systems from unintentional damage and data from unauthorized disclosure or modification and access to sensitive areas must be strengthened."	55
		"Per our review of access to the IIM system ('IRMS'), we noted that the access request forms, which document assigned user codes and passwords are not stored in a secure location at the OTFM. Without strong controls to safeguard against unauthorized access to assigned user codes and passwords, the risk of unauthorized modifications to trust data is increased."	55
Report Date	Report Title	Problem	Page
		"Per our review of access to IRMS, we noted that there are inadequate controls of user codes and passwords including: user codes are not routinely removed for terminated or transferred employees; passwords are not changed on a regular basis; complete documentation does not exist to readily identify the owner of each user code. Without strong controls related to the access to sensitive Trust systems, the risk of unauthorized modifications to trust data is increased. Additionally, any unintended modification may be difficult to detect and correct without an adequate audit trail."	56

		"In the event of a disaster, an agreement exists to perform remote processing of IIM applications in Scottsdale, Arizona. However, the disaster recovery plan has not been tested since the conversion of the Unisys A17 to the Unisys NX Clearpath Server. It has been almost two years since the last test was performed. Without a proven recovery plan, the possibility exists that Trust operations would not resume within a reasonable period of time in the event of a disaster."	56
January 2001	Independent Auditors Report on the Financial Statements for Fiscal Years 1999 and 1998 for the Office of the Special Trustee for American Indians Tribal and Other Special Trust Funds and Individual Indian Monied Trust Funds Managed by the Office of Trust Funds Management	"[I]nadequacies in various Department of the Interior ("DOI") Indian Trust Fund accounting systems and subsystems controls and records caused the systems to be unreliable."	5
		"Records management is inconsistent and inadequate to ensure the proper filing and safekeeping of Trust Fund records to support trust financial activity, however, a mandatory documents policy has been adopted and verification of these mandatory documents will be checked in the centralized pre-posting review procedure."	14
		"Periodic reviews of system reports were not being performed. Specific, clearly defined information security policies and procedures for system security monitoring do not exist."	49
Report Date	Report Title	Problem	Page
		"User codes are not routinely removed for terminated or transferred employees. Passwords are not changed on a regular basis. Complete documentation does not exist to readily identify the owner of each user code."	49

		"Per our review of access to the OSC and SEI operated systems, we noted that the access request forms, which document assigned user codes and passwords are not stored in a secure location. Without strong controls to safeguard against unauthorized access to assigned user codes and passwords, the risk of unauthorized modifications to trust data is increased."	50
May 2001	Independent Auditors Report: Bureau of Indian Affairs Financial Statements Fiscal Year 2000	"BIA controls over its Operations Service Center automated information systems did not comply with OMB Bulletin 98-08, and BIA had not fully implemented the recommendations made in our April 1997 audit report 'General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs' (No. 97-I-771) and our June 1888 report 'Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs' (No. 98-I-483)."	13

2. **Office of the Inspector General Reports: Recommendations**

Five of the OIG reports discussed above recommended that:

1. the BIA "ensure the Bureau has the ability to efficiently and effectively recover operations in order to reduce both the risk of financial loss and the level of disruption to the Bureau and its Area offices. Recovery from government agencies with compatible systems is a viable option; however, tests of such arrangements should be performed to identify potential compatibility or capacity problems." OIG Report No. 97-I-196, Report of Independent Public Accountants on Internal Control Structure (December 39, 1996) at 37.

2. the BIA "evaluate options to increase the level of security controls implemented. Those controls identified in the observation should be taken into consideration. We also suggest that only those individuals with system administrator designation be allowed to reset passwords." Id. at 38.

3. the BIA "evaluate the cost/benefit of developing a segregated test and production environment on the Unisys. Separate environments will assist in maintaining the integrity of the data and the production application. Procedures should be implemented requiring the review of all application changes by a technical individual other than the programmer. At a minimum, each of the two IIM programmers should review the work of the other and document approval before Data Management places the application into production." Id. at 38.

4. "Because the OTFM is currently in the process of investigating, and later implementing a new IIM system, a computer conversion is again anticipated. Due to the complexity and volume of the information carried on the IIM system, a systems consultant should be considered. A consultant would have the benefit of not having every day tasks to

perform for the OTFM and could dedicate time to an initial and ongoing needs analysis, investigating and presenting alternative systems and rating their advantages and disadvantages. The consultant would also be able to assist in the implementation of the system and the training of OTFM personnel. Before another conversion is undertaken, the OTFM should complete a detailed plan noting who will be involved, what each individuals' responsibilities will be, and their corresponding deliverables." Id. at 39.

5. The BIA "ensure that: 1. The automated information system security function is elevated organizationally to at least report directly to the Director, Office of Information Resources Management; is formally provided with authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments; 2. A system security program is developed and documented which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-130, Appendix III, and that policies and procedures are implemented to keep the system security program current; 3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified." OIG Report No. 97-I-771, Audit Report: General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (April 30, 1997) at 10.

6. the BIA "ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical ADP positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred." Id. at 12.

7. the BIA "develop and implement policies to classify Bureau's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130, Appendix III." Id. at 13.

8. the BIA "ensure that: 1. Sufficient staff are provided to adequately monitor all visitor activities; 2. Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room." Id. at 15.

9. the BIA "ensure that policies are developed and implemented which match personnel files with system users periodically, that user Ids are deleted from the system for users whose employment has been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate." Id. at 16.

10. the BIA "ensure that a higher priority is given to moving the applications that reside on the UNISYS computer to the IBM computer." Id. at 17.

11. the BIA "ensure that policies and procedures are developed and implemented which

clearly identify the individuals responsible and accountable for application development and changes." Id. at 18.

12. the BIA "ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized." Id. at 20.

13. the BIA "ensure that access and activities of the Center's system programmer are controlled and monitored by security staff and that RACF controls are established to protect system resources." Id. at 22.

14. the BIA "ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility." Id. at 24.

15. the BIA "1. Ensure that risk assessments are conducted in accordance with guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk; 2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy; 3. Determine the risks associated with local area network applications and personal computer databases which contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures." OIG Report No. 98-I-336, General Controls Over Automated Information Systems, Royalty Management Program, Minerals Management Service (March 24, 1998) at 10.

16. the BIA "1. Evaluate Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity levels are greater than the position sensitivity levels of the employees who are performing the work; 2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work; 3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic followup background check are performed as required." Id. at 14-15.

17. the BIA "establish controls to enforce Program policy which requires employees to sign security awareness statements before access to system resources is approved by the Installation Automated Information System Security Officer." Id. at 17.

18. the BIA "1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource; 2. Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource." Id. at 20.

19. the BIA "implement controls to enforce Program policy that default user Ids and passwords are to be removed from the automated information system when commercial off-the-shelf software is implemented." Id. at 22.

20. the BIA "1. Evaluate the current Program policy which only recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment; 2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data." Id. at 25.

21. the BIA "1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy; 2. Document procedures which require that users' access levels be reviewed periodically or that employees be recertified to ensure that the levels of access granted are appropriate for the duties assigned to the users." Id. at 27.

22. the BIA "evaluate the need to deviate from the Departmental standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts." Id. at 29.

23. the BIA "enforce its procedures for authorizing, approving, and testing client server application software before the software is moved into production." Id. at 30.

24. the BIA "1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data; 2. Improve detection controls by ensuring that management or the Installation Security Officer reviews server security logs periodically." Id. at 33.

25. the BIA "ensure that the upgraded version of RACF is implemented immediately if the Program is granted a waiver from consolidating its mainframe operations with another mainframe operation." Id. at 35.

26. the BIA "1. Evaluate acquiring system verification and auditing software; 2. Implement the system options to record activities in the SYSLOG during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management; 3. Evaluate the available SMF record typed and implement procedures to ensure that critical SMF logs are reviewed periodically and that Program management addresses the problems identified." Id. at 38.

27. the BIA "update the disaster recovery plans to include all mission-critical systems." Id. at 40.

28. the BIA "develop and implement written policies and procedures defining appropriate system security, physical access, documentation standards, password controls and disaster recovery plans including, but not limited to the following: a) System generated security reports are periodically run and reviewed for unusual activity; b) Immediate revocation of access upon termination, retirement or transfer of an employee (should be part of employee check out procedure); c) Periodic review of issued cards and access levels for staff changes; d) Granting access only to those individuals whose job function requires access on a routine basis; e) Documentation that discloses trust system user codes and passwords be in a secured location at all times; f) Passwords be periodically changed; g) Every user code be readily identified to a specific user; h) A full test of the disaster recovery plan should be performed as soon as possible." OIG Report No. 01-I-434, Independent Auditors Report on the Financial Statements for Fiscal Years 1998 and 1997 for the Office of the Special Trustee for American Indians Tribal and Other Special Trust Funds and Individual Monies Trust Funds Managed by the Office of Trust Funds Management (May 22, 2000) at 56.

29. the BIA "establish and implement policies and procedures to ensure that physical inventories of property, plant, and equipment are accurate and complete; acquisitions and disposals are timely and accurately recorded; adequate supporting documentation is maintained; completed construction projects are timely transferred to the appropriate accounts; depreciation expense is timely and accurately recorded; and errors in the Fixed Asset Subsystem are timely identified and corrected." OIG Report No. 01-I-385, Independent Auditors Report on the Bureau of Indian Affairs Financial Statements for Fiscal Year 2000 (May 11, 2001) at 7.

30. the BIA "establish and implement the controls necessary to ensure that adjusting journal/accounting entries are properly recorded in the appropriate general ledger control accounts and that financial information integrity reviews, reconciliations, and corrections are performed to ensure the accuracy and reliability of reported financial information." Id. at 9.

31. the BIA "develop and implement procedures to strengthen the reported internal control weaknesses over automated information systems." Id. at 13.

32. The BIA "establish and implement policies and procedures for conducting periodic condition assessment surveys and estimating deferred maintenance needs, including the requirement that the data and methodologies used to compute the estimate be documented, reviewed, and approved at the appropriate management levels." Id. at 15.

33. The BIA "establish and implement stewardship and performance measure management systems that include the control procedures necessary to ensure the timeliness, completeness, reliability, and availability of stewardship and performance measure information, including all supporting documentation and listings." Id. at 17.

34. The BIA "develop and implement procedures that ensure compliance with the Chief Financial Officers Act of 1990, Debt Collection Improvement Act of 1996, OMB Circular A-11, Prompt Payment Act, and Federal Financial Management Improvement Act of 1996, including managerial cost accounting management and reporting requirements." Id. at 21.

C. General Accounting Office Reports

The next series of reports assessing the state of Interior's IT Security were the two issued by the GAO. Those: (1) "evaluate the Department of the Interior's effort to acquire and develop" TAAMS, GAO Report GAO/AIMD-00-259, Indian Trust Funds: Improvements Made in Acquisition of New Asset and Accounting System But Significant Risks Remain (September 2000) at 1; and (2) "evaluate the Department of Interior's High-Level Implementation Plan . . . for improving its management of the Indian trust funds and resources under its control." GAO Report No. GAO/AIMD-99-53, Indian Trust Funds: Interior Lacks Assurance That Trust Improvement Plan Will Be Effective (April 28, 1999) at 1.

1. General Accounting Office Reports: Findings

With respect to IT security, the GAO found that:

Report Date	Report Title	Problem	Page
April 1999	Indian Trust Funds: Interior Lacks Assurance That Trust Improvement Plan Will Be Effective	Interior "did not clearly specify all of BIA's requirements, including its functional, security, and data management requirements. For example: While Interior stated that the system 'shall include safeguards against conflicts of interest, abuse or self-dealing,' it did not define these terms. A definition of these terms in the context of Indian trust operations is necessary to design and determine the adequacy of proposed system safeguards and approaches. In discussing system security, Interior (1) specified an inappropriate technology encrypting data, (2) did not specify how long system passwords should be, and (3) did not require password verification features."	11

		"In acquiring its new TAAMS service, Interior did not carry out critical risk management steps. First, Interior did not develop a risk management plan. Without this plan, Interior has no disciplined means to predict and mitigate risks, such as the risk that the service will not (1) meet performance and business requirements, (2) work with Interior's systems, and/or (3) be delivered on schedule and within budget."	12
September 2000	Indian Trust Funds: Improvements Made in Acquisition of New Asset and Accounting System But Significant Risks Remain	"Interior has not yet completed actions designed to enhance overall trust fund management, including its efforts to revamp policies and procedures for the entire trust management cycle and to address long-standing internal control weaknesses."	2
Report Date	Report Title	Problem	Page
		"[T]here were serious flaws in the way Interior was planning and conducting its system tests (which verify that a system satisfies functional requirements) and its first set of user acceptance tests (which verify that the system operates correctly with operational hardware and meets user needs). Without following a disciplined testing processes, Interior could not ensure the successful implementation of TAAMS. In particular, test plans were flawed because they were designed with the assumption that no errors would be found. They also did not include tests of invalid and unexpected conditions – known as boundary testing . . . . Furthermore, some obvious problems/defects that occurred as the tests were conducted were ignored because testers assumed that the unanticipated results were attributable to eccentricities or malfunctions of the computing platform rather than to defects in the system being tested."	7

		"Interior has not reengineered business processes which TAAMS is being designed to support even though these processes use an older and a very different system environment. Until it does so, Interior will not be able to maximize the benefits that can be gained from TAAMS, and it may perpetuate outmoded ways of doing business."	12
		"Many of the internal controls now being reviewed by Interior – such as segregation of duties, supervisory review, system security, and project payment management – relate to requirements that should have been defined early in the TAAMS effort. Because they were not defined early by Interior, TAAMS was developed based on the current control environment, long known to be inadequate. As a result, like the policies and procedures effort, Interior may have to modify TAAMS after deployment to accommodate new controls, thereby increasing development risks and costs. Also, until adequate internal controls are in place to ensure the accuracy, availability, and completeness of trust fund data, Interior will not be able to fully ensure the integrity of TAAMS on an ongoing basis."	15
Report Date	Report Title	Problem	Page
		"Not having a complete information systems architecture to guide TAAMS and other projects under its improvement effort will continue to be a major challenge for Interior."	16
		"While the absence of an architecture does not guarantee the failure of TAAMS or other system modernization efforts, it does greatly increase the risk that Interior will spend more money and time than necessary to ensure that its systems are compatible with each other and in line with business needs."	17

1. **General Accounting Office Reports: Recommendations**

In each of its reports, the GAO recommended that:

1. "before making major investments in information technology systems to support trust operations, the Secretary direct the Chief Information Officer to develop an information systems architecture for Indian trust operations that (1) provides a high-level description of Interior's mission and target concept of operations, (2) defines the business functions

to be performed and the relationships among functions; the information needed to perform the functions; the users and locations of the functions and information; and the information systems needed to support the department's business needs, (3) identifies the improvement projects to be undertaken, specifying what they will do, how they are interrelated, what data they will exchange, and what their relative priorities are, and (4) details specific standards and approaches that will be used to build or acquire systems, including hardware, software, communications, data management, security, and performance characteristics." GAO Report No. GAO/AIMD-99-53, Indian Trust Funds – Interior Lacks Assurance That Trust Improvement Plan Will Be Effective (April 1999) at 14.

2. "the Secretary of the Interior direct the Chief Information Officer to (1) clearly define and validate functional requirements, security requirements, and data management requirements, (2) develop and implement an effective risk management plan, and (3) ensure that all project decisions are based on objective data and demonstrated project accomplishments, and are not schedule driven." Id. at 14.

3. "the Secretary of the Interior direct the Assistant Secretary for Indian Affairs to work with the Special Trustee for American Indians to do the following before phase II of TAAMS: Examine and revise business processes supported by TAAMS; Properly develop and implement data conversion plans; Evaluate and revise policies, procedures, and internal controls relating to TAAMS; ensure that top trust fund managers across the department participate in this effort; and ensure that any needed modifications to TAAMS are made and tested." GAO Report No. GAO/AIMD-00-259, Indian Trust Funds: Improvements Made in Acquisition of New Asset and Accounting System But Significant Risks Remain (September 2000) at 20-21.

4. "the Secretary of the Interior direct the Chief Information Officer to do the following before Phase II of TAAMS: A) Evaluate existing software development and acquisition processes against the Capability Maturity Models developed for these activities by the Software Engineering Institute; implement disciplined processes where they are lacking; and regularly assess progress in this regard; B) Ensure that contractors used by Interior to develop software systems have implemented discipline software development processes; C) Define and manage the requirements that TAAMS should meet using accepted processes. Once the requirements have been adequately defined, perform a gap analysis to assess whether TAAMS is capable of providing the necessary functionality and what modifications, if any, are necessary to address Interior's needs. If modifications are needed, then Interior should develop the cost, schedule and performance impacts of making those modifications." Id. at 21.

5. "the Secretary . . . develop an information system technology architecture for trust fund operations. In the interim, we recommend that the Secretary direct the Chief Information Officer to (1) perform an analysis of the infrastructure necessary to support the TAAMS application and ensure its adequacy and (2) ensure that TAAMS can interface with TFAS and MMS systems." Id. at 21.

D. **Computer Security Report Card**

On September 11, 2000, the House of Representatives Subcommittee on Government

Management, Information, and Technology, Committee on Government Reform, chaired by Congressman Stephen Horn (R-Ca), issued its Computer Security Report Card. The Report Card represented the first ever comprehensive study of computer security throughout the Executive Branch. See Computer Security Report Card Hearing Before the Subcomm. on Gov't Management, Information, and Technology of the Comm. on Gov't Reform, House of Representatives, 106th Cong., 1-2 (2000) ("Computer Security Report Card"). Horn assigned grades based on self-reported answers to Subcommittee and General Accounting Office (GAO) questions. Id. at 12 [25] The Subcommittee's overall grade for the federal government's information security was a "D-." Id. at 16.

1. **Computer Security Report Card: Findings**

Of the 24 major federal agencies studied by the Horn Subcommittee, the Social Security Administration (B) and the National Science Foundation (B-) earned the highest grades. The Commerce, Education, State, Housing and Urban Development departments and the Agency for International Development, received grades of C or C-, and the Defense and Treasury departments, as well as the Environment Protection Agency, General Services Administration and NASA, received grades of D+, D and D-, respectively. Among those agencies receiving an incomplete grade due to lack of information were the Department of Energy, the Nuclear Regulatory Commission, the Department of Transportation and the Federal Emergency Management Agency. Computer Security Report Card at 7-8.[26]

---

[25] The Report Card focused on six areas of computer security including: (1) Security Program Plan (the implementation and monitoring of agency-wide security program to manage risk); (2) Access Control (the ability to limit or detect unauthorized logical or physical access to computer resources); (3) Change Control (the ability to control unauthorized programs or program changes); (4) System Software (the ability to limit and monitor access to programs that control or secure computers and applications; (5) Segregation of Duties (the ability to limit individual responsibilities for key aspects of computer-related operations; and (6) Service Continuity (the ability to implement a plan to continue critical operations and protect data if unexpected events occur). Computer Security Report Card at 15.

[26] An agency received a grade of "incomplete" if it did not fully complete a report. Computer Security Report Card at 7-8.

The Office of Personnel Management received an F grade, along with the Justice, Labor, Agriculture, Health and Human Services Departments, the Small Business Administration and the Department of the Interior.[27]

In addition to the letter grade, Horn's committee rated the various agencies on a point basis. Out of a possible high of 100 points, Horn's grades were based on whether agencies had established entity- wide security programs (29 points), access controls (26 points), the ability to continuously provide service even when unexpected events occur (18 points), checks on unauthorized change in computer programs (12 points), limiting access to sensitive operating system files (12 points) and segregation of duties controls (3 points). Computer Security Report Card at 12. Interior received the lowest score of 17 while Labor received the second-lowest score of 38.[28] Id. at 16.

E. **SeNet International, Inc. Reports**

On December 7, 1999, then-Special Advisor to the Assistant Secretary for Indian Affairs Dominic Nessi commissioned SeNet[29] to assess and evaluate the state of BIA's IT Security.[30] The original contract was subsequently modified on 5 separate occasions. As set out in its final version,

---

[27] The Report Card does not individually score the Bureau of Indian Affairs.

[28] John Dyer, CIO of the Social Security Administration, and a witness at the September 11 hearing, attributed his agency's relative success to "a longstanding tradition of assuring the public that their personal records are secure stakes are simply too high." Computer Security Report Card at 143. Department of the Interior CIO Daryl White testified that Interior was "making substantive progress to improve [its] computer security posture," id. at 155, but that Interior's "ability to completely implement an adequate computer security program is strongly dependent upon the availability of necessary resources." Id.

[29] SeNet,founded in June 1998, performs work for both government and commercial clients See June 1, 2001 Interview of SeNet President Toly Kozushin at 8.

[30] The original contract and modifications indicate that it was executed between Digicon and the National Business Center (a component of the DOI) on behalf of the BIA. According to the Department of Justice, "[A] representative from SeNet advised that [Digicon and SeNet] are unrelated and that there is merely a subcontracting relationship between the two entities." November 6, 2001 Letter from Department of Justice Deputy Director Commercial Litigation Branch Sandra Spooner to Special Master Alan Balaran at 1.

SeNet was tasked to:

- Perform an Independent Verification and Validation (IV&V)[31] of TAAMS Disaster Recovery Program, and deliver an IV&V Report for a December 17, 1999 restoration test with recommendations, and an IV&V Report for the June 1, 2000 restoration test with recommendations;

- Develop a TAAMS Disaster Recovery Plan and Disaster Recovery Procedures, and deliver a TAAMS Disaster Recovery Plan and a set of TAAMS Disaster Recovery Procedures;

- Examine and evaluate the physical security of Artesia's Data Center located in Addison, Texas, and deliver a Data Center Physical Security Report with recommendations;

- Examine, analyze and evaluate security policies and controls at the Artesia Data Center, and deliver a report on the adequacy of the Artesia Data Center network topology and boundary protection controls;

- Review and evaluate TAAMS end user access security, and deliver a TAAMS User Access Policies and Procedures report;

- Perform an analysis of TAAMS performance, and deliver a TAAMS Performance Test Results briefing and a TAAMS Wide Area Network bandwith requirements and topology recommendations;

- Propose solutions for improving TAAMS performance and implement an improvement pilot program at one regional office, and deliver a Proof of concept implementation and test report and a Pilot implementation report;

- Perform miscellaneous TAAMS-related activities, including attend TAAMS status meetings;

- Review BIANet Architecture and Performance, and deliver a report on BIANet Architecture and performance with recommendations, and document the status of the BIANet at the 12 BIA Regional Offices and the Albuquerque, New Mexico and Reston, Virginia Data Centers; and

- Assist in BIA security analysis and planning, and deliver BIA Information Security Policies and Procedures, System Security Plans for LRIS, IRMS, TAAMS, BIANet and major office LANs, and Proposed BIA Information Security Implementation Plan.

---

[31] IV&V in an abbreviation of "Independent Verification & Validation."

See Order No. NBCWOP00179, Modification 5.[32]

In addition to generating the reports specified in the contract, SeNet also produced the following reports:

- Physical Security Implementation Guidelines, BIA Data Center, Reston, VA;
- Information Technology Risk Assessment Security Survey Report;
- Department of Interior Bureau of Indian Affairs Office of Information Resources Management Final Trust Systems Backup Procedures; and
- Vulnerability Analysis IRM Ely Parker Building, Reston, VA.

All told, SeNet generated 18 reports describing IT security – 13 of which noted specific problems. These reports analyzed:

- "[T]he security requirements," the "management, operational, and technical controls in place and planned for meeting those requirements," and the "responsibilities and expected behavior of all individuals who access" TAAMS. TAAMS System Security Plan (July 6, 2001) at 3. A draft of this report was issued on February 15, 2001.
- "[T]he security requirements," the "management, operational, and technical controls in place and planned for meeting those requirements," and the "responsibilities and expected behavior of all individuals who access" the Integrated Records Management System ("IRMS"). IRMS System Security Plan at 3 (June 30, 2001). A draft of this report was issued on February 15, 2001.
- "[T]he security requirements," the "management, operational, and technical controls in place and planned for meeting those requirements," and the "responsibilities and expected behavior of all individuals who access" the Land Records Information System ("LRIS"). LRIS System Security Plan (June 30, 2001) at 3. A draft of this report was issued on either February 28, 2001 or May 21, 2001.[33]
- "[T]he security requirements for" the BIA Wide Area Network, the "management,

---

[32] The total cost of the contract was $995,505.22. Id. at 3.

[33] The cover date on the draft report indicates a February 28, 2001 issuance date; the interior pages indicate that the report was issued on May 21, 2001.

operational, and technical controls in place and planned for meeting those requirements," and the "responsibilities and expected behavior of all individuals who access" the network. BIANet System Security Plan (June 30, 2001) at 2. A draft of this report was issued on April 19, 2001.

- "[T]he security requirements for" the Reston Local Area Network, the "management, operational, and technical controls in place and planned for meeting those requirements," and the "responsibilities and expected behavior of all individuals who access" the network. Reston LAN System Security Plan, (June 30, 2001) at 2.

- Protecting the BIA "data center in Reston, VA against unauthorized physical access" and "environmental and disaster prevention measures." Physical Security Implementation Guidelines BIA Data Center, Reston, VA, (August 18, 2000) at 4. Drafts of this report were issued in February and August of 2000.

- "[P]rotect[ing] the TAAMS Data Center in Addison, TX against unauthorized physical access." Physical Security Implementation Guidelines TAAMS Data Center, Addison, TX, (June 16, 2000) at 4. A draft of this report was issued in either late May 2000 or early June 2001.[34]

- "[I]ssues related to the Security Current State" and the "efforts [that] are required to reach the Security Desired State" at the Bureau of Indian Affairs. Information Technology Risk Assessment Security Survey Report, (January 4, 2000) at 4.[35]

- "Establish[ing] and maintain[ing] adequate and effective security safeguards to ensure data privacy, confidentiality, integrity, and operational availability of all systems that process, store, or transmit information" and "preserv[ing] information processing integrity, reliability and availability to ensure that the data are accurate and relevant to meet commercial and administrative requirements." Information Technology Security Program, (February 15, 2000) at 5.

- "[P]olicies and procedures for controlling the operational aspects of users' access to the TAAMS application and its database." Trust Asset and Accounting Management System (TAAMS) User Access Security Policies, Guidelines and Procedures, Version 1.0, (July 6, 2001) at 4. A draft of this report was issued on February 2, 2001.

---

[34] The cover date on the draft report indicates a May 26, 2000 issuance date, while the interior pages of the draft indicate a June 10, 2001 issuance date.

[35] A Risk Assessment is a document containing "findings, recommendations and project information resulting from a security study" that "document[s] issues related to the Security Current State and to define the efforts that are required to reach the Security Desired State." IT Risk Assessment at 4.

- "AS 400 and connectivity restoration activities, and Comdisco's and ATS's preparedness" for an Independent Verification and Validation of the TAAMS Disaster Recovery Program. Trust Asset and Accounting Management Systems (TAAMS) Independent Verification and Validation of TAAMS Disaster Recovery Program, (July 3, 2000) at 4.

- "[H]ow the data on [OIRM Trust data systems] will be backed up and restored (in the context of the official disaster recovery plan)." Department of Interior Bureau of Indian Affairs Office of Information Resources Management Final Trust Systems Backup Procedures,(May 17, 2001) at 1 .

- "[T]he effectiveness of security controls implemented to protect Trust data processed and stored on IT resources located within the boundaries of the Ely Parker building." Vulnerability Analysis IRM Ely Parker Building, Reston, VA, (July 15, 2001) at 12.

1. **SeNet International Reports: Findings**

In the Risk Assessment, the BIA Security Program, the TAAMS User Access Security Report and the IV&V of TAAMS Disaster Recovery, SeNet issued the following findings:

General Problem	Report	Section Name and No.	Description of Problem	Page No.
Access Control	IT Risk Assessment	2.1.3: Network Resources	"Access to most network resources is protected only by user Ids and passwords. No other access control mechanisms, such as firewalls, VPNs, strong authentication, are implemented."	7
	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"Users are assigned multiple Ids/Passwords, which forces them to write them down ('yellow sticker' syndrome). This leads to potential misuse of user accounts."	10
General Problem	Report	Section Name and No.	Description of Problem	Page No.

	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"Accounts remain active after users change roles or leave the agency. This problem is amplified because the 'disenrollment' is much more difficult to enforce, and BIA has found it difficult to cross reference its employee data (obtained from OPM via FPPS) with their systems' user accounts information. Some requests for deleting inactive accounts (e.g., IIM) come from the application owner (OTFM) directly to application support staff bypassing the security officer."	10
	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"The security officer can not always positively verify authorizing signatures. Sometimes a telephone conversation is used as a means of verification, which is questionable at best. Sometimes forms come to a system administrator without the authorization signature."	11
	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"Additional logistics problems due to interaction between the BIA and the outsourcing organization exist in administering accounts on 'outsourced' resources."	11
	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"There is no indication on the form that the person was (or was not) cleared for the position of public trust."	11
	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"The paper-based enrollment/disenrollment process is time consuming and bulky."	11

	IT Risk Assessment	2.6.1: Identification, Authentication and Authorization	"As indicated, authentication relies on user selected passwords. We found that there is no consistent policy regarding password 'strength' or rotation requirements, though for some systems this is changing. . . . This situation is a serious vulnerability as it allows users to select easy passwords and never change them. Vulnerability testing conducted at the OIRM facility proved this to be the case with many users. Furthermore, some user accounts are shared which makes tracking of security violations virtually impossible."	11
General Problem	Report	Section Name and No.	Description of Problem	Page No.
	IT Risk Assessment	2.6.4: Perimeter Protection	"Weak perimeter protection is by far the most common cause of security breaches (intrusions) by outsiders. Our findings indicate that the current situation presents a serious security risk. . . . This makes the Albuquerque network and its resources vulnerable to intrusion from within BIA/DOI, from all connected non-DOI agencies, and from the Internet at large. This risk is exacerbated by the fact that the DOINet functions as an ISP for a number of Government agencies and is connected to MAE-East and MAW-West National Access Points, thus opening the network, for all practical purposes, to the world."	12
	IT Risk Assessment	3.2: Primary Domain Controller	"Anonymous logins are allowed to the ftp [36] service."	18

[36] XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX.

	IT Risk Assessment	3.2: Primary Domain Controller (PDC)	"A simple test revealed that the [Primary Domain] account . . . had a trivial password. We were able to log into the system using this account and have complete, unrestricted access. . . . After expanding the XXXXXXXXXX were ran it through a password cracker . . . . The cracker broke XXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX. . . . Many of the passwords were trivial - for example, 'passwd' was very common was well as last/first names and other common English dictionary words."	20
	IT Risk Assessment	3.7: IBM P390	"Attempting guest access via the XXXXX failed. The response was [ ]. This could assist a potential intruder to guess the names of users who are defined on the system and proceed by guessing their passwords."	25
	IT Risk Assessment	3.5: IDEAS server	"[A]nonymous login is accepted" XXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX."	22
	IT Risk Assessment	3.10.: Web Server 1	"TheXXXX allows anonymous login" to the XXXXXXX."	27
General Problem	Report	Section Name and No.	Description of Problem	Page No.
	IT Risk Assessment	3.12.: Netware Servers XXXXXXXXXX XXXXXXXX XXXXXXXXX	"Some accounts do not have passwords XXXXXXXXXXXXXXXXX. Many accounts do not have a secure password (common dictionary words, first/last name combinations etc.). Many accounts are not required to change password or the interval is greater than 60 days. Some user accounts are assigned access rights beyond their own space in the system. These weaknesses are relatively easy to fix by adopting and enforcing stricter policies. The built in tools plus free utilities can be used effectively to weed out these vulnerabilities."	29-30

	IT Risk Assessment	3.13.: Winframe	"XXXXXXXXXXXXXXX we were able to download the list of locally defined users. It appears that many users have not logged in to this system since their accounts were created almost two years ago. This might allow an intruder to get in without being noticed. . . . Although XX[37] access is protected by a userID and password, a potential intruder will have many user accounts to try before giving up. Based on our experience with the XXXX, the remote intruder will have a fairly easy job to break into this system."	30
	TAAMS User Access Security	2. ATS Security Implementation for TAAMS	"[A]s of October 2000, no specific actions were taken towards the implementation of boundary protection on any BIANET node."	34
	TAAMS User Access Security	AS/400 Password Policy	"There is no limit to the number of times users can fail to log into TAAMS. TAAMS accounts are not locked out due to failed login attempts."	35
General Problem	**Report**	**Section Name and No.**	**Description of Problem**	**Page No.**
	TAAMS User Access Security	AS/400 Password Policy	"Currently, the IT security office assigns TAAMS application account Ids and passwords based on a format that is simple to guess. A user, which was given a password by the IT security office, can easily guess the account Ids and passwords assigned to fellow employees and use their identity to log into TAAMS."	36

[37] XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

	TAAMS User Access Security	Client Application Security	"Other than password protected BIOS[38] and password protected screen savers, TAAMS workstation provides no security controls. If BIOS password protection is not configured, upon power up the TAAMS application's icon is automatically displayed on the desktop. No LAN or workstation logon are required to display the application's icon."	36
Data Sensitivity	IT Risk Assessment	2.3: Data Sensitivity	"The required level of information confidentiality varied between different systems. Although each interviewee could properly estimate the sensitivity of the data he or she was responsible for, there is no formal procedure to assign security classification to an application or to establish an objective measure of sensitivity."	9
Training	IT Risk Assessment	2.4: Security Awareness, Training and Education	"The BIA OIRM does not have an information security awareness training program in place. Some information is given to new employees as a part of orientation process."	9
System Config-uration	IT Risk Assessment	2.6.2: System Configuration Maintenance	"Our findings indicate that there are no consistent standards of system security configurations. In some cases many system configuration parameters are left at their default settings. . . . Our general observation is that the sophistication of a system's security configuration was determined primarily by the system administrator's knowledge and awareness. The lack of standard procedures makes major systems vulnerable to external and internal abuse. For example, the BIA primary DNS [Domain Name System] server is being used as an unofficial web site for a private company."	11-12
General Problem	Report	Section Name and No.	Description of Problem	Page No.

[38] "BIOS" is an abbreviation for Basic Input Output System, which is an "essential set of routines in a PC, which is stored on a chip and provides an interface between the operating systems and the hardware." <http://www.techweb.com/encyclopedia/defineterm?term=BIOS> (Visited Nov. 9, 2001).

	IT Risk Assessment	2.6.6: Content Filtering	"There are no known installations of WEB and e-mail content filtering software at any of the BIA computing facilities. Interviews with OIRM management, however, indicated a certain level of concern about potential abuse of internet access privileges and e-mail by some BIA employees and contractors, which can be mitigated by using COTS[39] packages."	13
	IT Risk Assessment	3.2: Primary Domain Controller	"Web Service is enabled with a major vulnerability in the form of an executable script file."	18
	IT Risk Assessment	3.3: Backup Domain Controller	"For acting as a XXXXXXXXXXXXXXXXXX XXXXXXXXX the only service required is XXXXXXX. The other services, unless absolutely needed, make the XXXX vulnerable to their associated risks."	21
	IT Risk Assessment	3.4 Network Management System XXXXX XXXXX	"The number of available services is too high for a system with such specific purposes. . . . This system was also found to be configured with a weak XXX[40] community string, this allowed [sic] to retrieve details about the system. . ."	21
	IT Risk Assessment	3.5 IDEAS server	"As is the case with other systems, the availability of unused/unnecessary services greatly increases the risk of unauthorized access."	22
	IT Risk Assessment	3.5 IDEAS Server	"We found that web service is enabled on the server. The fact that the XX is still using the default server page indicated that this service is not in use. Using XX remote admin capabilities a hacker could easily change the home page. Further more [sic], this version of XXXXXX contains theXXXXXXXXX vulnerability which can be used by an attacker to create files anywhere on the system if they have the XXX correct file permission to do so."	24
General Problem	Report	Section Name and No.	Description of Problem	Page No.

[39] COTS ("Commercial-Off-The-Shelf") is defined as "ready-made merchandise that is available for sale." *TechEncyclopedia*, (visited Oct. 17, 2001) <http://www.techweb.com/encyclopedia/defineterm?term=COTS>.

[40] XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

	IT Risk Assessment	3.6: Lotus Notes Server	"Access to the web service on this system is user ID and password protected, although the banner indicated 'Enter username for XXXXXXXXX XXXXXXXXXXXXXXX' which reveals the system's purpose to unauthorized users. Likewise, connection the XXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX XXXXXX which tells the potential intruder what package is used for e-mail, and thus narrows down his/her search for vulnerabilities."	25
	IT Risk Assessment	3.8: SMTP Notes E-mail Server	"Web access is protected by user ID and password, but the prompt reveals the system's identity. . . ."	25
	IT Risk Assessment	3.10.: Web Server 1	"XXXXXXXXXXXXXXXXXX which can be used to view any file in the system. . . . The XXXXXXXXXXXXX files indicate that XXXXXXX is active on this server. This potentially allows any remote user to modify web content on this server."	27
	IT Risk Assessment	3.11. Web Server 2	"The XXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX allows an intruder to search for various files on the system XXXXXXXX. The XXXXXX XXXXXXXXXXXXXXXXXXX indicates that XXXXXXXXX is running. It may allow users to upload files to a XXXXX directory or create it if it does not exist. If the file permission on this directory are unrestricted, remote users can upload and execute arbitrary files."	28
	IT Risk Assessment	3.11. Web Server 2	"The system is configured with a weak XXX community string (actually the installation default). This can be used to provide a significant amount of information on the system. . . ."	29
	IT Risk Assessment	3.12.: Netware Servers XXXXXXXXXX XXXXXXXXXX XXXXXXX	"The servers are part of a BIA-wide Novell network which consists of over 100 servers spread through all 12 regions. An intruder can attempt to break into these servers from any attached PC throughout the BIA network (perhaps the entire DOI network)."	29
General Problem	Report	Section Name and No.	Description of Problem	Page No.

	IT Risk Assessment	3.14.L DNS Server	"It is evident that this system has many ports open in addition to the ones needed for the DNS function. The XXXXXX allows anonymous access and the directory allows upload of files. The XXXXXX web vulnerability was designed to display information about the Web server environment, but it parses data requests too liberally and thus allows a person to view a listing of arbitrary files on the Web server host. The XXXXXXXXXXXXXXX allowed a remote user to execute any command on the target system with the same privileges as the web server. Interestingly, the following page shows up when pointing to a browser to the XXXXXXX address. It was possibly set up by the contractor who installed the XXXXXX or by someone who hacked into it later."	31
	TAAMS User Access Security	Citrix Security Implications	"[E]liminating the need to obtain the client application software in order to run TAAMS increases vulnerability and must be compensated by stricter security controls on the XXX servers."	33
	TAAMS User Access Security	Citrix Security Implications	"Another security problem is theXXXXXXXXXX XXXXXXXXX XXX platform used by the 15 XXX servers. XXX is known to have many security vulnerabilities."	33
	TAAMS User Access Security	Citrix Security Implications	"Finally, because the client application executes on the XXX server, users must be reminded that by turning off their workstation they will not terminate the application. It will continue to execute on the XXX server. The only way to terminate the application is by closing it via the main menu. This may pose a security risk if a power outage occurred at the user's site while users are accessing TAAMS. . . . If the user leaves the work area and shortly thereafter the power is resumed, the user's instance of the TAAMS application is still running on the Citrix server and can be easily made available again on the desktop. Since the application is already running, intruders do not need XXX and TAAMS user ID or password to launch the application. After reinitializing the XXXX (which was closed when the power was interrupted), intruders can continue the TAAMS session by using the credentials of the authorized user who was interrupted by the power outage."	33-34
General Problem	Report	Section Name and No.	Description of Problem	Page No.

Encryption	IT Risk Assessment	2.6.7: Privacy and Encryption	"Encryption is not used at the BIA for any purpose, including e-mail. Considering the sensitive nature of information and the geographical dispersion of BIA users, the use of encryption technology would be highly advisable."	14
	TAAMS User Access Security	Data Encryption	"ATS did not develop and implement additional encryption beyond what is provided as a default by COTS tools . . . used in the TAAMS environment."	37
Auditing/ Logging	IT Risk Assessment	2.6.8: Security Monitoring, Logging and Reporting	"In general we find that while capabilities are available, they are not utilized and need to be augmented to make this task more efficient. . . . What we found though is that logs are not reviewed in a consistent way: while the Unisys security event logs are generated nightly and reviewed on a daily basis, logs of other systems are only inspected when something goes wrong and used primarily as troubleshooting tools. We find this to present a risk to BIA operations because unauthorized activity can go undetected indefinitely."	14
	IT Risk Assessment	2.6.9: Incident Reports	"BIA currently does not have a procedure for responding to information security related incidents, such as an attempt to gain unauthorized access to information resources, or an evidence of tempering with data."	15
	IT Risk Assessment	3.12.: Netware Servers XXXXXXXXX XXXXXXXXX XXXXXXXXX	"Not all security features of NetWare are employed (e.g. packet signature) or fully utilized - event logs are not routinely reviewed for security violations. In fact no one is in charge of following up on security events that do get noticed (and there is no formal procedure for doing so in the first place)."	29
Policies & Procedures	IT Risk Assessment	2.7: Policies and Procedures	"This issue is of utmost importance to the BIA security posture. . . . In the process of data gathering for this Report, SeNet was provided with several documents related to Information Security Policies [ ] none of which could constitute a comprehensive (and approved!) policies document."	15
General Problem	Report	Section Name and No.	Description of Problem	Page No.

	IT Risk Assessment	3.12.: Netware Servers XXXXXXXX XXXXXXXX XXXXXXXX	"Security procedures regarding these servers are lacking or not uniformly enforced. For example, users can get a waiver from following the requirements to change their password once in three months. We were told that certain users got SUPERVISOR rights just because they demanded it and not because they have compelling need for it."	29
Remote access	BIA Security Program	2.4.4: Remote Access	"Both dial-in lines and the Internet are used to provide remote access to BIA resources. Both types of connections can be eavesdropped, but it is much more likely to happen on Internet connections."	14
Disaster Recovery	IV&V of TAAMS Disaster Recovery	3.4: Status of earlier recommend-ations	"A review of the client application test procedure should be conducted to verify that it covers all components of the TAAMS application." – "Not Implemented: Billings did not review or approve the script prior to the test."	11
	IV&V of TAAMS Disaster Recovery	3.4: Status of earlier recommend-ations	"BIA should develop scripts to simulate load testing and run them during the June 21st recovery test." – "Not Implemented: Still Valid."	11
	IV&V of TAAMS Disaster Recovery	3.4: Status of earlier recommend-ations	"BIA may want to consider scheduling and running the next test at a secondary Comidsco facility to verify that the facility and its personnel can also support TAAMS requirements." – "Not Implemented: Given Carlstadt's high availability, the likelihood of a Chicago restoration is low. However, this recommendation is still valid."	12
General Problem	Report	Section Name and No.	Description of Problem	Page No.

	IV&V of TAAMS Disaster Recovery	3.4: Status of earlier recommend-ations	"Additional disaster recovery tests on ATS' XXXX hardware should be conducted . . . . A study should be conducted to identify which XXXX redundancy and fault tolerance technologies employed by the XXXX can be tested and verified. These tests should be conducted at the Addison, TX site prior to the June 21st test." – "Not implemented: These tests were not conducted. On several occasions, SeNet discussed these types of tests, as well as XXXX redundancy and fault tolerance technologies with IBM representatives (Section 5.5a of the DRP addresses these XXXX features.) However, because the maintenance agreement with IBM prohibits ATS from physically accessing the XXXX (except for the On/Off switch), it may not be feasible to conduct such tests. The BIA will have to rely on manufacturer test data."	12-13

SeNet also produced five System Security Plans based on standards set out in NIST Special Publication 800-18. See June 11, 2001 Interview of Jeremy Katz at 27. These System Security Plans exposed security deficiencies found in the BIANET, IRMS, LRIS, TAAMS and Reston LAN systems. Specifically, SeNet reported the following:

Section No. and Name	System	Problem Description	Page No.

1.9.2:Existing or planned means of dial-up access	BIANET	“Dial up into such network devices is needed in case of a circuit(s) failure. When the circuit that connects a site to the BIANET (and to the remote management station – NAS help desk) fails, the only way to connect to the router or XXXX[41] from a remote location is via a modem. For diagnostic purposes it is important to have this dial-up communication channel available, however OIRM has decided not to implement this feature.”	16
1.9.3: Existing or planned connections to the Internet	BIANET	“The Internet is accessible to all BIANET users. Five non-secure gateways provide the physical connection to the DOINET, which currently serves as an ISP for BIA users. Because of the non-secure nature of the connection (e.g. no firewalls are installed) the BIANET and all the computing resources connected to it (e.g. BIANET’ XXXX, IRMS’ UNISYS NX, LRIS’ IBM 3090) are extremely vulnerable to attacks over the Internet.”	16
	IRMS	“The Internet is accessible to all BIANET users. Five non-secure gateways provide the physical connection to the DOINET, which currently serves as an ISP for BIA users. Because of the non-secure nature of the connection (e.g. no firewalls are installed) the BIANET and all the computing resources connected to it (e.g. BIANET’ XXXX, IRMS’ UNISYS NX, LRIS’ IBM 3090) are extremely vulnerable to attacks over the Internet.”	9-10
	LRIS	“The Internet is accessible to all BIANET users. Five non-secure gateways provide the physical connection to the DOINET, which currently serves as an ISP for BIA users. Because of the non-secure nature of the connection (e.g. no firewalls are installed) the BIANET and all the computing resources connected to it (e.g. BIANET’ XXXX, IRMS’ UNISYS NX, LRIS’ IBM 3090) are extremely vulnerable to attacks over the Internet.”	13
Section No. and Name	System	Problem Description	Page No.

[41] XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

	TAAMS	"The Internet is accessible to all BIANET users. Non-secure gateways provide physical connections to the DOINET, which serves as an ISP for BIA users. Because of the non-secure nature of the Internet connectivity (e.g. no firewalls are installed) the BIANET and all its resources including the XXXX and the XXXX servers that support TAAMS are extremely vulnerable to attacks."	8-9
	Reston LAN	"[T]he Internet is accessible to all Reston LAN users. Each of the five BIANET hubs provides connections to the DOINET, which serves as an ISP for BIA users. Because of the non-secure nature of the connection (e.g., no firewalls are installed), the BIANET and all the computing resources connected to it (e.g., TAAMS XXXX, IRMS UNISYS NX, LRIS Multiprise 3000) are extremely vulnerable to hacker attacks over the Internet."	10-11
1.9.5: Documentation for system's custom-written software	IRMS	"None of the documentation listed above, except for the source code, is available for review. This documentation, if exists, cannot be located, and the version of code currently executing can not be verified."	10
	LRIS	"Because of a room and personnel change, all LRIS documents, manuals, and interoffice memos dating back to 1980 were boxed up (in over twenty boxes), and moved to another office on the same floor (room 4553, Main Interior building). Locating specific documents or manuals within the boxes may be a time consuming effort because the exact contents of each box is unknown. The documents will remain boxed up until a replacement LRIS manager is designated by OTR. According to the previous LRIS manager most of the documentation listed above is available inside the boxes."	13-14
	Reston LAN	"There is no custom written software for the Reston LAN devices. However, the following documentation is required for proper LAN operations and maintenance. . . . Not all documentation listed above is maintained by and available from OIRM."	12
Section No. and Name	System	Problem Description	Page No.

1.9.6: Security software modules	BIANET	"No custom security software modules were developed specifically for the BIANET. The only BIANET software-based security control in use on BIANET devices is the login ID and password on BIANET routers and the RAS server. XXXXX devices on the BIANET have no authentication requirement for administration, even though these devices are addressable from the Internet. This is a major security gap as it allows Internet hackers to easily telnet into BIANET XXXXXX devices and modify them. No other software-based security controls, such as encryption, firewalls and tunneling were implemented on the BIANET. OIRM is in the initial planning process for installing firewalls in the five BIANET hubs. Another firewall is planned for the TAAMS data center in Dallas, TX. Once funds are approved, OIRM will solicit requests for proposals for firewall acquisition and installation. Firewall rules will be available for after the firewalls are fully configured and tested. Virtual Private Networks (VPNs), Internet content filtering, and intrusion detection devices are also under consideration for implementation by OIRM during FY2002 (depending the availability of funds). "	18
	IRMS	"No custom security software modules were developed for IRMS. Only XXXXX operating system security and the password management component of XXXX security package are used to authenticate users. Currently, there are no plans to create new security software modules for IRMS."	10-11
	LRIS	"Some custom security software modules were developed for LRIS to authenticate users login to the application. . . . Since TAAMS is planned to replace LRIS, there are no plans to create new, or strengthen existing LRIS security software."	14
	Reston LAN	"Two software-based security control are in use on Reston LAN devices. The first control is the login ID and password for servers (Novell, NT and Unisys) and account ID and password for the router and XXXXX. The second control is Norton anti-virus software, which is installed on all BIA desktop computers and servers. No other software-based security controls, such as encryption, firewalls, or intrusion detection, are implemented on the Reston LAN."	12
Section No. and Name	System	Problem Description	Page No.

1.9.7: Existing and planned physical security controls	BIANET	"Other sites located BIANET equipment in an un-secure location, accessible to individuals who were neither authorized nor cleared by the BIA."	18
	IRMS	"There are no plans for additional security or environmental controls for the Reston data center."	11
	TAAMS	"Out of the 5 security levels specified in the GSA's 'Vulnerability Assessment of Federal facilities' report published on June 28, 1995, TAAMS data center was classified by the BIA as level 2. . . . . None of the building entrances is protected by an alarm system."	10-12
1.10.1: Interconnected systems and identifiers	BIANET	"There is a total of over 42 Major Applications, residing on mainframe and midrange computers that are supported by the BIANET. . . . However, it is important to note that as of March 2001, only a small portion of these systems (both BIA and DOI) had a security plan in place . . . . In general, most of these systems have been in operation for two decades, and documentation describing how these systems were designed and implemented is not readily available. OIRM, the organization responsible for the BIANET does not maintain any such documentation. OIRM's role is to provide the infrastructure to support the interconnection between systems. Securing these interconnections is part of the services provided by the infrastructure and is a major concern for OIRM. The contents of the information exchanged over the BIANET between interconnected systems becomes a concern when sensitive and highly-sensitive information passes through BIANET equipment and circuits."	19-20
	IRMS	"The RDRS and TFAS systems do not have an OMB A-130 compliant security plan in place."	12
	TAAMS	"Currently, there are no OMB A-130-compliant security plans for either MRM Financial System or TFAS. . . . Currently, all file transfers use anonymous XXX and the data is transferred in clear text. No login is required and destination directories on the TFAS system and TAAMS where files are stored, have no access security controls. The Service Bureau and BIA are aware of the security breaches created by this implementation."	12-13
Section No. and Name	System	Problem Description	Page No.

	Reston LAN	"The Reston LAN is the interconnecting media for over 200 BIA employees. . . . Not counting Major Applications owned by other DOI agencies, there is a total of 42 interconnected Major Applications, residing on several mainframe and midrange computers. In addition, BIA operates hundreds of General Support systems. . . . [I]t is important to note that as of June 2001, only a small portion of these systems (both BIA and DOI) had a security plan in place. BIA is planning to complete the security plans for all its major applications by the end of 2001."	13-14
1.10.4: Security concerns and considerations regarding interconnections	BIANET	"OIRM's [sic] have three security concerns for its BIANET in three major areas: physical protection of BIANET equipment at the over 200 BIA sites served by the BIANET; access security protection for its routers via telnet or dial-up connections; and protecting BIANET equipment and computers on the BIANET from Internet attacks. Additional concerns are in the areas of environmental controls and BIANET availability. . . . Telnet and dial-up protection are provided by the use of user ID and passwords, but it is limited only to the routers. XXXX devices, even though they are addressable, are not configured for authentication. . . . In the area of BIANET boundary protection, OIRM started the process of evaluating firewalls from various vendors. The configuration, rules, or vendor of the proposed firewalls have not been determined yet (as of February 2001)."	20-21
	IRMS	"There are several security concerns regarding the interconnection of IRMS and the OTFM and MMS systems. The first concern is the anonymous connection. It does not require an ID or a password to establish the connection. The second concern is that no security controls were implemented on destination directories, where personal and financial information is stored. Because these systems are accessible from the XXXX, the combination of no password protection and no access rights restriction makes these systems extremely vulnerable for unauthorized access and data modification for financial gain. BIA, MMS, OTFM and ATS are all aware of these security deficiencies. Because IRMS is planned for a phase out, there are no plans to redesign and strengthen the security software component of the interconnection protocol."	12-13
Section No. and Name	System	Problem Description	Page No.

	TAAMS	"1. The anonymous XX connection does not require an ID or password to establish the connection. 2. No security controls were implemented on destination directories, where personal and financial information is stored. Because these systems are accessible from the XXX, the combination of no password protection and no access rights restrictions makes these systems extremely vulnerable to unauthorized access and data modification. BIA, MMS, OTFM and the Service Bureau are all aware of these security deficiencies."	13-14
	Reston LAN	"With adequate physical and environmental controls in place, OIRM's security concerns for the Reston LAN focus on implementing user access security, preventing unauthorized access to LAN resources, and working with BIA system owners and other DOI agencies on improving security for interconnecting systems. OIRM is in the process of developing a user access security plan, and is planning on implementing strong authentication, as well as strengthening overall security by installing firewalls and intrusion detection systems."	15
1.12.1: Sensitivity of information and need for protective measures	BIANET	"Several BIANET applications require the transmission of sensitive and highly sensitive information over BIANET circuits. . . . Currently, no special security measures other than authentication are used by the BIANET and its applications. The Cisco routers used by OIRM can be configured to encrypt/decrypt all data transferred over the BIANET. This approach will ensure the confidentiality of information but will significantly decrease network performance. . . . Because OIRM is currently not using encryption on its Cisco routers, and because the owners of major applications did not implement encryption at the application level, OIRM cannot guarantee the confidentiality of information transmitted over its facilities. In addition, because of lack of funding no special measures to ensure non-repudiation and data integrity were implemented by OIRM. . . . Currently, because of lack of funding, OIRM is not taking any proactive measures to increase the reliability and availability of BIANET equipment that is under its control."	21-22
Section No. and Name	System	Problem Description	Page No.

	IRMS	"IRMS receives, processes and stores information required to make payout distributions. . . . Such applications must operate in an environment that provides integrity, confidentiality, and availability. In addition, the fraud-prone nature of financial systems requires non-repudiability of transactions. The fact that many individual Indians and tribes depend on timely distribution of funds puts a premium on plausibility and availability of the data, as does the fact that Indian trust funds are currently a subject of litigation and active public interest. Therefore, the IRMS system was classified as highly sensitive in all categories."	13
	LRIS	"LRIS data is extremely sensitive. . . . Unauthorized access to, modification, creation or the removal of LRIS records may cause financial damage to individuals and tribes. The ability of BIA to manage Indian affairs was questioned in the U.S. Congress, the media, and recently in the US District Court. Any breach of security on any of the BIA's systems, or interconnected systems in other agencies, will damage BIA's credibility."	16-17
	TAAMS	"TAAMS trust information must be protected from unauthorized access. Therefore, user access to the TAAMS system must be secured and the TAAMS data center in Addison, TX must provide a physically secure environment for the sensitive information that it stores. . . . Unauthorized access to, modification, creation or the removal of TAAMS records may cause financial damage to individuals and tribes. The ability of BIA to manage Indian affairs was questioned in the U.S. Congress, the media, and recently in the US District Court. Any breach of security on any of the BIA's systems, or interconnected systems in other agencies, will damage BIA's credibility.	14-15
	Reston LAN	"To comply with the Privacy Act of 1974 and the Computer Security Act of 1987, some of the information transmitted over the Reston LAN must be protected. . . . The only type of information that does not require protection is general Web browsing and personal e-mail messages."	15-16
Section No. and Name	System	Problem Description	Page No.

1.12.3: Estimated risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information transferred over the system	BIANET	"The magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information transferred over the BIANET can be very high. Individuals and tribes will suffer financial damages if trust data is accessed and modified without proper authorization. The US Government may suffer financially if unauthorized users create or modify trust data for financial gain. Congress' level of confidence in BIA's ability to properly manage Indian affairs will be damaged if data was lost, misused or modified without authorization."	22-23
	IRMS	"The magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information stored on or transferred to IRMS can be very high. Individuals and tribes will suffer financial damages if trust data is accessed and modified without proper authorization. The US Government may suffer financially if unauthorized users create or modify trust data for financial gain. Congress' level of confidence in BIA's ability to properly manage Indian affairs will be damaged if data was lost, misused or modified without authorization. Loss or misuse of information may result in claims from individual Indians, payers and recipients of rents and royalties. Loss of trust fund interest income, penalty interest for late payments, frauds, bad publicity, and the cost of litigation are some of the damages that can result from not properly securing the IRMS operational environment."	14
Section No. and Name	System	Problem Description	Page No.

	LRIS	"The magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information stored on or transferred to LRIS can be very high. Individuals and tribes will suffer financial damages if trust data is accessed and modified without proper authorization. The US Government may suffer financially if unauthorized users create or modify trust data for financial gain. Congress' level of confidence in BIA's ability to properly manage Indian affairs will be damaged if data was lost, misused or modified without authorization. Loss or misuse of information may result in claims from individual Indians, payers and recipients of rents and royalties. Loss of trust fund interest income, penalty interest for late payments, frauds, bad publicity, and the cost of litigation are some of the damages that can result from not properly securing the LRIS operational environment. Unavailability of the system could result in inability to meet payment obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system also contains financial information, which could result in late payments and loss of public confidence. The system requires access during working hours only."	18-19
	TAAMS	"The magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information in the system is very high. Individuals and tribes could suffer financial damages if trust data are tempered with. The US Government may suffer financially if unauthorized users create or modify trust data for financial gain."	15
	Reston LAN	"The magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information transferred over the Reston LAN can be very high. Individuals and tribes will suffer financial damages if trust data is accessed and modified without proper authorization. The US Government may suffer financially if unauthorized users create or modify trust data for financial gain. The Public's level of confidence in BIA ability to proper manager Indian affairs may be damaged if data were lost, misused or modified without authorization."	16
2.1.1: Data of last risk assessment	BIANET	"A risk assessment for the entire BIANET was not conducted."	24
Section No. and Name	System	Problem Description	Page No.

	IRMS	"A risk assessment for the IRMS system in the Albuquerque NM data center was conducted during the week of November 29, 1999. A risk assessment at the new site in Reston VA has not been conducted."	15
	LRIS	"In the last six years no risk assessment was conducted on LRIS. There is no information on this subject for prior years. As for the Multiprise 3000 that hosts LRIS and the NBC/PS Data center, the most recent complete Risk Assessment was performed in November of 1996. An incremental Risk Assessment covering the addition of the Multiprise computer system and additional FFS, Model 204, and Adadbase applications (including LRIS) was performed in December of 2000. The next complete Risk Assessment for the NBC/PS Data Center is scheduled to be completed by July of 2001.	20
	TAAMS	"Risk assessment of TAAMS operations has not yet been conducted."	16
	Reston LAN	"BIA has not conducted a vulnerability and risk assessment of the Reston LAN. The assessment shall be conducted after funds are approved."	17
2.1.5: Date of next risk assessment	BIANET	"There are no current plans for a BIANET risk assessment. However, BIANET is a high priority effort for OIRM. It will be conducted as soon as funds become available."	24
	IRMS	"There are no current plans for another IRMS risk assessment."	15
	LRIS	"The next Risk Assessment is planned for July 2001."	22
	TAAMS	"The Risk Assessment is planned for midyear 2001."	16
	Reston LAN	"Vulnerability and risk assessments of the Reston LAN is [sic] being planned for April-June 2001 in conjunction with the Indian Trust Data Protection Analysis - Reston Facility Project."	17
2.2.1: Security Audits on new installations	BIANET	"A security audit was not conducted on any of the BIANET sites. No new BIANET node installations are planned. Security audits will be conducted as soon as funds become available."	24
Section No. and Name	System	Problem Description	Page No.

	IRMS	"The OIG conducted an audit of the new Reston installation in October 2000. OIG did not publish a report yet. Based on prior OIG audits, security audit was most likely included in this audit. The Reston data center and the Unisys NX became operational at the end of November 2000, two months after the OIG audit, and most likely were not included in the audit."	16
2.2.2: Date of last security audit	IRMS	"The last published OIG report is dated July 1999 "	16
	LRIS	"The last management Control Review was conducted in July of 1998."	22
	Reston LAN	"A security audit of the Reston facility, including the data center, was conducted by SeNet Int. in April June [sic] 2001."	17
2.2.6: Date of next security audit	BIANET	"For the lack of funding, none scheduled at the present time."	25
	IRMS	"None scheduled at present."	17
	LRIS	"The next Management Control Review is scheduled to be complete by July of 2001."	23
	TAAMS	"None scheduled at present."	17
	Reston LAN	"None scheduled at present."	18
2.3.1: Who is responsible for enforcement of Rules of Behavior?	Reston LAN	"The user's immediate supervisor, the CIO, DAM, and BIA managers, and ultimately the Department of Justice, are responsible for enforcing the system's rules of behavior. OIRM does not have the authority needed to enforce these rules on individual users. OIRM and the BIA IT Security Office are responsible for issuing security policy guidelines but not for enforcing them. Rules of behavior for Reston LAN users are in the development phase."	18
2.3.2: Provide reference to the Rules of Behavior	BIANET	"There are no documented Rules of Behavior for users of the BIANET."	25
	IRMS	"There are no documented Rules of Behavior for users of IRMS."	17
	LRIS	There are proposed rules, but no rules	24
	TAAMS	There are proposed rules, but no rules	17
Section No. and Name	System	Problem Description	Page No.

	Reston LAN	"Currently, there are no documented Rules of Behavior for users of the Reston LAN."	18
2.3.3: Consequences of inconsistent behavior	BIANET	"Not Defined."	25
	IRMS	"From verbal reprimand to removal from duty and even criminal prosecution."	18
	LRIS	"Employees who violate BIA's policy regarding rules of behavior for LRIS may be subject to disciplinary action at the discretion of BIA's management. Actions may include a verbal or written reprimand, removal of system access for a specific period of time, reassignment to other duties, up to and including removal from service, depending on the severity of the violation."	24
	TAAMS	"Employees who violate BIA's policy regarding rules of behavior for TAAMS may be subject to disciplinary action at the discretion of BIA's management. Actions may include a verbal or written reprimand, removal of system access for a specific period of time, reassignment to other duties, up tp and including removal from service, depending on the severity of the violation."	18
	Reston LAN	"Not Defined."	18
2.3.4: Stipulations concerning work at home, dial-up, etc.	BIANET	"No specific documented stipulations address work at home, dial-in access, connection to and use of the Internet, use of copyrighted material, and use of Government equipment."	25
	IRMS	"No specific documented stipulations were established to address work at home, dial-in access, connection to and use of the Internet, use of copyrighted material, and use of Government equipment."	18
	LRIS	"As for the proposed LRIS Rules of Behavior, no specific stipulations have been established to address work at home, or LRIS access via the Internet or dial-up lines. Access over dial-up lines is supported for BIA and contractor LRIS users. LRIS rules of behavior prohibit users from downloading LRIS data onto client workstation, and from removing printed reports out of LRIS designated areas."	24
Section No. and Name	System	Problem Description	Page No.

	TAAMS	"No specific stipulations have been established to address work at home, or TAAMS access via the Internet or dial-up lines. By publishing the TAAMS client application on the XXXX servers, and by making these servers accessible via the Internet, TAAMS became available for Internet users. It is a relatively simple effort to install the XXXX client on a notebook or a home computer (the software and installation instructions are available on the XXXX Web site). After installing the XXXX client, if the IP address of any of the XXXX servers is known, an unauthorized user can configure a workstation to connect to the XXXX server and to display the login screen. Access over dial-up lines is not currently supported for BIA and contractor TAAMS users. TAAMS rules of behavior prohibit users from downloading TAAMS data onto client workstations, and from removing printed reports out of TAAMS designated areas."	18
	Reston LAN	"No specific documented stipulations were established to address work at home, dial-in access, the use of the Internet, the use of copyrighted material, and the use of Government equipment."	18
2.3.5: How do users get Rules of Behavior	BIANET	"Currently there are no documented rules of behavior to hand out to BIANET users."	25
	IRMS	"Currently there are no documented rules of behavior to hand out to IRMS users."	18
	LRIS	"Dissemination of these rules is the responsibility of departmental managers and security points of contact for client organizations."	24
	Reston LAN	"Currently there are no documented rules of behavior to hand out to Reston LAN users."	19
2.4.1.1: Initial Security Requirements	BIANET	"No initial security requirements were outlined."	26
2.4.1.2: Security controls, evaluations, etc. for development and procurement	BIANET	"No security controls, evaluation and test procedures have been specified for the procurement and implementation of BIANET. The contract with MCI and NAS did not specify any security requirements for the system or for contractor personnel."	26
Section No. and Name	System	Problem Description	Page No.

	LRIS	"Information regarding security controls, evaluation and test procedures for the development of LRIS is not available. The application was developed almost twenty years ago and there are no records for the RFP, the contract, or the system requirement specifications."	25
	TAAMS	"No security controls, evaluation and test procedures have been specified for the development of TAAMS."	19
	Reston LAN	"No security controls, evaluation and test procedures have been specified for the procurement and implementation of the LAN. Security controls were specified by NBC for the data center facility, but the specifications are not available for review. There were no evaluations and test procedures for the development and procurement of data center security and physical controls."	19
2.4.1.4: Were security requirements identified in the acquisition specifications?	BIANET	"No security requirements were identified in the RFP, or the contracts with the various vendors."	26
	IRMS	"OIRM acquired, installed and activated the password management component of the Infoguard security package. The other three components are under consideration by OIRM."	18
	LRIS	"No security requirements were identified and included in the acquisition specifications of the COTS components. Only standard security controls in COTS components are used."	25
	TAAMS	"No security requirements were identified in the RFP, the contract, or Modification #9 for COTS components."	19
	Reston LAN	"With the exception of physical security, no security requirements were identified in the RFP, or the contracts with the various construction, equipment, and service contractors. STG Inc. of Gaithersburg, MD submitted a proposal to NBC for the implementation of physical security controls."	19
2.4.1.5: Risk Assessment before commencement?	BIANET	"No."	26
	TAAMS	"No."	19
Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"No."	19

2.4.2.1: During design, were security requirements specifically identified?	BIANET	"Since the BIA purchased only COTS product, specific security requirement documents were not developed."	26
	TAAMS	"Specific security requirement documents were not developed."	19
	Reston LAN	"Security requirements were not developed for the Reston LAN"	19
2.4.2.2: Has the system been under Change Control Process?[42]	BIANET	"No. The system was not placed under change control even after it became operational."	26
	LRIS	"No. LRIS is not under change control process."	26
	Reston LAN	"No. The LAN was not placed under change control even after it became operational."	19
2.4.2.3: Process to update security requirements?	BIANET	"No specific process for updating BIANET security requirements exists."	26
	IRMS	"No specific process for updating IRMS security requirements exists."	19
	LRIS	"No process for updating security requirements exists. Since LRIS will be replaced by TAAMS, no additional changes are made to the application."	26
	TAAMS	"No process for updating security requirements exists."	20
	Reston LAN	"Such a process does not exist. Reston LAN security requirements have not been specified."	20
2.4.2.5:When was system certified/accredited?	BIANET	"The BIANET was never officially certified/accredited."	26
2.4.2.8: Post development security controls	IRMS	"References to Infoguard acceptance test reports are not available."	19
Section No. and Name	System	Problem Description	Page No.
	LRIS	"No new security controls were added to the application. No additional changes are made to LRIS because it is scheduled to be replaced by TAAMS."	26

[42] Change Control Process is "used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes." NIST Special Publication 800-18 at 32.

	TAAMS	"No new security controls were added to the application. Some physical access security controls have been added. No acceptance tests were performed on the new controls."	21
	Reston LAN	"No new security controls were added to the Reston LAN since it was delivered to OIRM in June of 2000."	20
2.4.3.1: Process of logging and reviewing system security activities	BIANET	"There are no documented processes, guidelines or procedures for logging and reviewing BIANET security incidents. All BIA security incidents, including BIANET must be reported to, the security officer of OIRM."	27
	IRMS	"There are no documented processes, guidelines or procedures for logging and reviewing IRMS security incidents. All BIA security incidents, including IRMS must be reported to Dr Ryl, the security officer of OIRM. . . . Log analysis is performed whenever the security officer suspects improper activities or login attempts. There is no periodic analysis of system security logs and no written procedures on how to perform such analysis."	19
	Reston LAN	"There are no documented processes, guidelines, or procedures for logging and reviewing LAN security incidents. The undocumented policy is that all BIA security incidents, including Reston LAN, must be reported to Dr Ryl, the security officer of OIRM."	20
2.4.3.4: What system security training classes are available? How often each person has to take 'refresher' course?	BIANET	"No formal end user security training is currently provided by OIRM. . . . Currently, OIRM does not provide security awareness training to its technical personnel responsible for operating, administering, and maintaining the BIANET. OIRM does not provide security training for its LAN administrators in sites connected to the BIANET."	27
Section No. and Name	System	Problem Description	Page No.

	IRMS	"No formal end user security training is currently provided by a central organization, such as the OIRM Security Office. Supervisors provide some training to new users, but it does not follow any standard. . . . Currently, OIRM does not provide security awareness training to its technical personnel responsible for operating, administering, and maintaining IRMS. OIRM does not provide security training for its LAN administrators in sites connected to IRMS."	20
	LRIS	"No end user security training is currently provided."	28
	TAAMS	"No end user security training is currently provided. . . . Currently, the Service Bureau does not provide security awareness training to its technical personnel responsible for operating, administering, and maintaining the TAAMS system. BIA does not provide security training for its LAN administrators in TAAMS sites."	22
	Reston LAN	"No LAN user security training is currently provided. . . . Currently, OIRM does not provide security awareness training to its technical personnel responsible for operating, administering, and maintaining the Reston LAN. OIRM does not provide security training for BIA LAN administrators in sites connected to the BIANET either. Plans and curricula for training are currently under development. Completion is projected for Q4 FY 2001."	21
2.4.3.5: Does SAT address unique security considerations?	BIANET	"A security-training curriculum for BIANET users and operators was not developed yet."	27
	IRMS	"A security training curriculum for IRMS users has not been developed yet."	20
	LRIS	"LRIS end user security training has not been developed yet. Service Bureau security training is not specific to LRIS."	28
	Reston LAN	"A security-training curriculum for Reston LAN users and administrators has not been developed yet."	21
2.4.3.6: User administration & access control	BIANET	"There are no such procedures in place. The BIANET does not manage or maintain user tests. Anyone who can physically access a computer attached to the BIANET is automatically granted access to BIANET services. User controls and administration is performed on the computer systems (e.g., servers, mainframes) that are connected to the BIANET rather than the BIANET."	28

Section No. and Name	System	Problem Description	Page No.
	LRIS	"The 'LRIS User Access Security Policies, Guidelines And Procedures' manual, which is currently under development, will specify LRIS user administration and access control procedures."	28
	Reston LAN	"There are no such procedures in place. The LAN Administrator is the only person who can grant access to NetWare LAN servers. OIRM maintains user lists for NetWare and NT LAN servers. Because most desktops connected to the LAN are Windows 98, there is no need to first log on to the desktop computer or to a LAN server in order to access, for example, the Internet."	21
2.4.3.7: Disposal of obsolete information on system	IRMS	"There are no written procedures for the disposal of obsolete or damaged media. EMC, the RAID system maintenance organization, removes failed hard drives, replaces them with new ones and keeps the failed ones for possible repair. This process is unacceptable because the data on failed hard disks is not destroyed prior to giving the drive to EMC. The same process applies to damaged and old tapes, which are replaced by Arcus Corp. OIRM does not destroy the data on tapes removed by Arcus. BIA is aware of this security breach and is in the process of finding a solution."	20
	TAAMS	"No formal procedures are in place. Obsolete and damaged media are currently stored in the data center."	22
	Reston LAN	"There is no such procedure."	21
2.4.3.8: Controls to ensure confidentiality of system data	IRMS	"The only user access security control used by IRMS is user ID and password. By itself, this control is insufficient to ensure confidentiality of data. It must be augmented by other controls, such as strong authentication."	20
	Reston LAN	"There are no confidential data stored on LAN devices. . . . However, some users may store highly sensitive information in their home directories on LAN servers and in e-mail messages."	21
3.1.1.1: Background Investigations.	IRMS	"Tribal IRMS users (known as 638 contractors) have not undergone security investigation."	22
	Reston LAN	"There is no requirement for LAN end-users to undergo and pass a background investigation by OPM. Security clearances for LAN users are handled by the agencies that employ these users."	22

Section No. and Name	System	Problem Description	Page No.
3.1.1.2: Drug certifications	BIANET	"No. Tests to determine the use of illegal drugs are not performed by either BIA or its contractors responsible for BIANET management."	29
	IRMS	"No. Tests to determine the use of illicit drugs are not performed on either BIA employees or its contractors responsible for IRMS operations."	22
	LRIS	"No. Tests to determine the use of illegal drugs are not performed by either BIA on its employees accessing LRIS, or NBC on its employees and subcontractors who operate, maintain, and use (e.g, help desk) the application."	30
	TAAMS	"No. Tests to determine the use of illegal drugs are not performed by either BIA on its employees accessing TAAMS, or the Service Bureau on its employees and subcontractors who develop and use (e.g., help desk) the application."	24
	Reston LAN	"No. Tests to determine the use of illicit drugs are not performed by the BIA."	22
3.1.1.3: Suitability determinations	BIANET	"However, since the contracts with NAS and MCI does not specify any personnel security requirements, no suitability determination is made for contractor personnel responsible for managing and maintaining the BIANET."	29
3.1.2.1: Who makes need determinations?	BIANET	"By default, all BIA employees have access right to the BIANET when they are given access rights to a computer that is physically connected to the BIANET."	29
	Reston LAN	"The user's supervisor submits a request form to OIRM security specifying which applications the user needs to access. Once approved by the security office, an account is created on the LAN server for the user. After the account is created, the user can access the requested application(s). No LAN access determination is specifically made, If the user is approved to access an application, LAN access is provided automatically."	22
3.1.2.2: Personnel authorized to approve system access	BIANET	"By default, every networked workstation can access the BIANET. When a supervisor assigns a networked workstation to a user, BIANET and Internet access are provided automatically."	29
	Reston LAN	"General use access to the LAN is granted automatically to all BIA employees without a need for a request or formal authorization."	23

Section No. and Name	System	Problem Description	Page No.
3.1.3.1: Procedure for extension, transfer, and reinstatement	BIANET	"Currently, no such procedures exist. The BIANET does not maintain users list. There are no documented procedures to address changes in the employment status (e..g, transfers, terminations, etc.) of BIANET management personnel. A procedure for at least changing router passwords is mandatory."	30
	IRMS	"Currently, there are no documented procedures to address changes in the employment status (e..g, transfers, terminations, etc.) of IRMS users."	23
	LRIS	"Currently, no such procedures exist for LRIS end users."	31
	TAAMS	"Currently, no such procedures exist."	25
	Reston LAN	"Currently, no such procedures exist. The Reston LAN does not maintain user list. There are no documented procedures that address how changes in the employment status (e.g., transfers, terminations, etc.) of OIRM and contractor LAN management personnel affect their access rights to the LAN."	23
3.1.3.2: Procedure for closing user accounts	BIANET	"For general user, no written procedures exist. If supervisors notify the OIRM security office about a termination or a transfer, the user's account for the major application is disabled or removed."	30-31
	IRMS	"No written procedures exist. When IRMS users terminate or transfer, their immediate supervisors supposed to notify the OIRM security office, which will disable the accounts."	23
	LRIS	"Currently, no such procedures exist."	31
	TAAMS	"Currently, no such procedures exist."	25-26
	Reston LAN	"No such procedures exists."	23
3.2.1.1: Physical security plan	BIANET	"BIA facilities housing BIANET equipment vary in their levels of physical access control implementation, from no controls or rudimentary mechanical locks to the most sophisticated security and environmental controls (e.g., the Reston BA data center). There are no available physical security plans for any of the BIA's facilities. When funding becomes available, OIRM plans to conduct a physical security survey of all BIA sites connected to the BIANET."	31

Section No. and Name	System	Problem Description	Page No.
	IRMS	"There is no physical security plan that describes what security and environmental controls were installed in the Reston data center and how these controls are integrated and managed to provide the desired level of security for IRMS. There is no test plan and test report that certifies that all controls operate properly."	24
	LRIS	"There is no facility security plan for the Denver Data Center."	33
	Reston LAN	"There is no physical security plan that describes what security and environmental controls were installed by NBC in the Reston data center and how these controls are integrated and managed to provide the desired level of security. There is no test plan and test report that certifies that all controls operate properly."	24
3.2.1.2: Guard hours	BIANET	"Of the over 100 BIA sites only sites that are located in Federal Buildings or buildings leased by GSA have guards on a 24*7 basis. All other sites do not have a guard."	31
	TAAMS	"No guards. After hours remote alarm monitoring."	26
3.2.1.3: On-Site or remote monitoring 24*7?	BIANET	"The vast majority of the over 100 BIA sites are not equipped with CCTVs or alarm systems, and are not monitored after hours."	31
	TAAMS	"The alarm system is monitored remotely after hours. CCTV is installed, and operational on a 24x7 basis to record all entries and exits to/from the computer room. However, the CCTV is not connected to the remote monitoring facility (ADT)."	26
3.2.1.4: Emergency doors	BIANET	"Differs from site to site. The vast majority of sites are small sites (e.g., agencies). They have only one door to the room or closet where BIANET equipment is located."	31
	IRMS	"There are two entrance doors into the data center. Both are used as regular and emergency doors. They are not serviced on a periodic basis. If and when there is a problem with any of the doors, the building engineer, who is on site during working hours, is called to correct the problem."	24

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"The data center has two entrance doors. Both are used as entry/exit and emergency doors. They are not serviced on a periodic basis. If and when there is a problem with any of the doors, the building engineer, who is on site during working hours, is called to correct the problem."	24
3.2.1.5: Are all alarms connected to a control alarm panel & linked to a staffed guard center?	BIANET	"Differs from site to site. . . . There are no plans to improve sites' physical security beyond what has already been implemented."	32
	IRMS	"There is no documentation describing the implementation of security controls in the data center available for review. . . . Most likely, all alarms are connected to a central alarm panel, and as required by local codes, fire alarms are sent to the fire station whenever smoke is detected in the building. . . . There are no plans to improve Reston's data center physical security beyond what has already been implemented.	24-25
	Reston LAN	"There is no documentation describing the implementation of security controls in the data center available for review. NBC did not provide this documentation."	24
3.2.1.6: Is biometrics[43] in place or planned?	BIANET	No/No	32
	IRMS	No/Yes, when funding is available	25
	LRIS	No/No	33-34
	TAAMS	No/No	26-27
	Reston LAN	No/No	24
3.2.1.7: Identification badges	BIANET	"The majority of BIANET sites (e.g., agencies) do not require identification badges."	32
3.2.1.8: Revoking Badges	BIANET	"There is no BIA-wide standard or policy for managing badges."	32

[43] Biometrics is the " biological identification of a person, which includes eyes, voice, handprints, voice, fingerprints and hand-written signature. Biometrics are a more foolproof form of authentication than typing passwords or even using smart cards, which can be stolen." *TechEnclyclopedia* <http://www.techweb.com/encyclopedia/defineterm?term=biometrics> (Visited Nov. 6, 2001).

Section No. and Name	System	Problem Description	Page No.
	TAAMS	"Currently, no procedures are in place."	27
	Reston LAN	"Specific information for the Reston facility is not available. Most likely standard DOI personnel security policies and procedures are used."	25
3.2.3.1: Smoke detector locations	TAAMS	"Only one smoke detector is installed inside the data center."	28
3.2.3.3: Zoned dry pipe sprinkler system	TAAMS	"No. No immediate plans to install, pending the availability of funds."	28
3.2.3.6: Protection from water	BIANET	"Only a few sites have water sensors connected to an alarm system."	33
	IRMS	"Water damage from burst or leaking supply and drain pipes is possible, and so is the damage from water seeping into the data center from adjacent rooms."	26
	LRIS	"[W]ater damage from burst pipes in room adjacent to the data center [is possible]."	35-36
	TAAMS	"[W]ater damage from burst pipes in rooms adjacent to the data center, or from a burst pope or sprinkler head in the data center's sprinkler system is possible."	28
	Reston LAN	"Water damage from burst or leaking supply and drainpipes is possible, and so is the damage from water seeping into the data center from adjacent rooms."	26
3.2.4.6: Emergency lighting	BIANET	"Differs from site to site."	34
	TAAMS	"No. In violation of local fire and safety codes, emergency lighting is not installed inside the two data center rooms. There Service Bureau and building management are in the process of installing emergency lighting as required by the codes."	29
3.2.5.1: Procedures to prevent unauthorized viewing of sensitive data	BIANET	"There are no documented procedures for handling this information."	34
	IRMS	"Currently, there are no procedures in place to prevent unauthorized personnel from viewing sensitive information displayed on authorized users' screens or printed on departmental printers."	27

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"There are no procedures is place to ensure that unauthorized personnel are prevented from viewing sensitive information displayed on authorized users screens or printed on departmental printers."	27
3.2.5.2: Procedures for investigation attempted breaches of the system	BIANET	"No written procedures for investigating attempts to breach system security exist."	34
	IRMS	"No written procedures for investigating attempts to breach system security exist. When the security office of OIRM suspects improper activities, or when security incidents are reported, it will investigate and review system logs. OIRM investigations are performed ad-hoc, depending on the circumstances."	27
	LRIS	"No written procedures on this topic are known to exist."	37
	TAAMS	"No written procedures on this topic are known to exist."	30
	Reston LAN	"No written procedures for investigating attempts to breach system security exist."	27
3.2.5.3: Procedures for visitors	IRMS	"The Reston site is currently in the process of developing written procedure for hosting visitors."	27-28
	TAAMS	"No such procedures are currently available. However, the Service Bureau is in the process of developing visitor control procedures."	30

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"The Reston site is currently in the process of developing written procedure for hosting visitors. Currently, visitors entering the Reston facility must identify themselves to the guard (a picture ID is required), log in their name, organization, BIA employee visited, and a time and date of the visit. Once confirmed by the visited BIA employee, a visitor is given a numbered visitor badge. Visitors do not have to be escorted by their host. Visitors are allowed into the data center only by an OIRM employee and must be escorted and monitored while inside the data center. These guidelines are used by BIA in the Reston facility, but they are not documented yet."[44]	27
3.2.5.4: Controls to ensure protected data are not accessible from any unprotected computer system or network	BIANET	"The only protected data is the router configuration and password. . . . BIANET XXXX devices have IP addresses but no password protection was implemented to secure then from XXXX attacks, therefore they are extremely vulnerable."	35
	IRMS	"Currently, there are no controls (such as firewalls and intrusion detection tools) in place to ensure that this type of information is not compromised from unprotected networks, like the Internet."	28
	TAAMS	"The Service Bureau's XXXX system and the XXXX servers are accessible from the Internet. There are no firewalls in place to mitigate risks associated with intrusion attempts via the Internet. Three-stage password protection XXXXXXXXXXXXXX is used to shield TAAMS data from intrusion attempts over the Internet. No additional controls have been implemented."	30
	Reston LAN	"Currently, there are no controls (such as intrusion detection tools) in place to ensure that this type of information is not compromised."	28
3.2.5.5: Who is authorized to approve access through the Internet to the system?	BIANET	"BIANET devices, such as routers, are accessible over the XXXX. No special authorization is required. BIANET administrators can telnet into the routers and login using the common password. XX employees can manage only the XXXXX devices."	35

[44] See Site Visit Report of the Special Master to The Office of Information Resource Management (March 12, 2001) at 1, describing the ease with which the Special Master and the Assistant Chief of ENRD, Department of Justice entered the OIRM facility.

Section No. and Name	System	Problem Description	Page No.
	IRMS	"IRMS is vulnerable to attacks over the XXXX because it does not have boundary protection."	28
	TAAMS	"TAAMS is accessible XXXXXXX. No special authorization or approval is required to access TAAMS from the Internet."	30
	Reston LAN	"When given access to a desktop computer that is connected to a LAN in any of BIA's sites, authorized (as well as unauthorized) users are automatically provided Internet access. There is no need for a special approval to access the Internet. Accessing Reston LAN resources (such as departmental servers and the Unisys NC) over the Internet to perform routine work is not supported. However, these resources are accessible from the Internet, and because no security measures are installed on the Reston LAN or the BIANET, they are vulnerable to attacks."	28
3.2.5.6: Mechanism for reporting suspicious/unauthorized activity	BIANET	"The OIRM Security Officer . . . is the focal point for reporting security incidents on the BIANET or any of the BIA computer systems connected to the network. No written procedures for such reporting exist."	35
	IRMS	"The OIRM Security Officer is the focal point for reporting security incidents on the BIANET or any of the BIA computer systems (e.g., IRMS) connected to the network. No written procedures for such reporting exist."	28
	TAAMS	"No intrusion detection tools are currently in use at the Service Bureau."	30
	Reston LAN	"The OIRM Security Officer . . . is the focal point for reporting security incidents on the Reston LAN or any of the BIA computer systems connected to the LAN. No written procedures for such reporting exist."	28
3.3.1: Help-desk response	BIANET	"No written security incident response procedures exist. The BIA does not provide 24*7 technical support for BIANET problems."	35
	IRMS	"No written security incident response procedures exist. The BIA does not provide 24*7 technical support for IRMS problems."	28
	TAAMS	"No security incident response procedures exist. 24*7 technical support is not available. The Service Bureau's Help desk is manned 6AM to 8PM Central Time."	30

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"No security incident response procedures exist. The BIA does not provide 24*7 technical support for LAN problems."	28
3.3.2:How to detect, handle, report problems	BIANET	"No formal procedures exist."	35
	IRMS	"No formal procedures exist."	28
	TAAMS	"No formal procedures exist."	30
	Reston LAN	"No formal procedures exist."	28
3.3.4: Procedures for handling incident reports	BIANET	"There are no formal procedures in place. Each case is investigated by OIRM."	35
	IRMS	"There are no formal procedures in place. OIRM security office investigates each incident based on the circumstances."	29
	TAAMS	"There are no documented procedures in place."	31
	Reston LAN	"There are no formal procedures in place."	29
3.3.5: Response to alerts and advisories	BIANET	"There are no written procedures for receipt and response to alerts and advisories. Whenever OIRM learns about new alerts and advisories (e.g., from vendors, user groups, knowledge-based web sites, etc.) OIRM will take ad-hoc actions to protect its resources."	26
	IRMS	"There are no written procedures for receipt and response to alerts and advisories. Whenever OIRM learns about new alerts and advisories (e.g., from vendors, user groups, knowledge-based web sites, etc.) OIRM will take ad-hoc actions to protect its resources."	29
	LRIS	"There are no documented procedures. An agreement with IBM is in place to keep the system running and updated."	40
	TAAMS	"There are no documented procedures. An agreement with IBM is in place to keep the system running and updated."	31
	Reston LAN	"There are no written procedures for receipt and response to alerts and advisories. Whenever OIRM learns about new alerts and advisories (e.g., from vendors, user groups, knowledge-based web sites, etc) OIRM will take actions to protects its resources."	29

Section No. and Name	System	Problem Description	Page No.
3.3.6: Application documentation	IRMS	"There is no documentation available for the IRMS application itself."	29
	TAAMS	"The Service Bureau keeps only select number of administration and operations manuals as references."	31
	Reston LAN	"There is no Vendor supplied software for LAN devices. Vendor-supplied application software documentation exits for major applications and support systems that are hosted on LAN servers. This documentation is owned and maintained by the respective system owner, not by OIRM."	29
3.3.7: Vulnerability information sharing	BIANET	"No formal procedures known."	36
	IRMS	"No formal procedures known."	29
	LRIS	"Although no written procedure is in place, in the event of a threat the Service Bureau system administrator would inform the BIA OIRM Security Office."	40
	TAAMS	"Although no written procedure is in place, in the event of a threat the Service Bureau system administrator would inform Norman Thornton of the BIA OIRM Security Office."	31
	Reston LAN	"No formal procedures known."	29
3.3.8: Quick response to incidents	BIANET	"No formal procedures are in place, however, when a security incident occurs and OIRM is notified, OIRM uses router filtering to disable to connection of the machine whose IP address was identified as the source of the incident."	36
	IRMS	"No such process is in place."	29
	LRIS	"No documented process could be identified."	40
	TAAMS	"No documented process could be identified."	31
	Reston LAN	"No such process is in place."	29
3.3.9: Disaster Recovery Procedures	BIANET	"The BIANET does not have a disaster recovery plan in place. Currently, there are no plans to develop one. The mashed topology of the ATM network, and MCI's guarantee for level of service as specified in the contract comprise BIA's assurances for disaster recovery."	36

Section No. and Name	System	Problem Description	Page No.
	IRMS	"The Reston data center does not have a disaster recovery plan in place."	29
	Reston LAN	"The Reston LAN does not have a disaster recovery plan in place. Currently, there are no plans to develop one."	29
3.3.10: Disaster Recovery warm/hot site	BIANET	"No alternate disaster recovery sites for BIANET hubs exist."	36
	Reston LAN	"No alternate disaster recovery sites for Reston LAN exist."	29
3.4.1: Controls to ensure unauthorized individuals cannot read, copy, alter or steal printed or electronic information	BIANET	"The only sensitive information is the router account ID and router and XXXXX configuration. . . .BIA's XXXXX devices are not protected by account Ids and passwords."	36-37
	IRMS	"Varies from site to site."	30
	Reston LAN	"It is the responsibility of individual system owner to establish security controls, which prevent unauthorized individuals from reading, copying, altering or stealing data or printed reports."	20
3.4.2: Audit trails	BIANET	"No audit trails for receipt of router configuration information exist."	37
	IRMS	"DMS database log shows status before and after each transaction, and a time stamp for each transaction. The system log is less detailed. It does not show the before-and-after text for each transaction."	30
	LRIS	"There are no audit trails in place for tracking hard copies of LRIS reports produced in field offices."	41-42
	TAAMS	"There are no audit trails in place for tracking hard copies of TAAMS reports produced in field offices."	32
	Reston LAN	"Audit trails for receipt of sensitive inputs/outputs are the responsibility of individual system owners. LAN devices have no sensitive inputs or outputs."	30
3.4.3: Procedures for transporting printed media	BIANET	"There are no procedures in place."	37
	IRMS	"There are no procedures in place."	30
	LRIS	"No procedures are in place for transporting hard copies of LRIS reports."	42

Section No. and Name	System	Problem Description	Page No.
	TAAMS	"No procedures are in place for transporting hard copies of TAAMS reports."	32
3.4.5.1: releasing sensitive information outside the original owner's care	BIANET	"Occasionally, router configuration information must be released to third parties. . . . There are no written procedures for controlling such information once it leaves OIRM."	37
	TAAMS	"Currently, there are no procedures in place to control this information once it is released."	33
	Reston LAN	"Reston LAN topology and configuration is not considered sensitive information. This information, in the form of topology diagrams and wiring lists, is maintained by OIRM and released only to third party repair and maintenance vendors as needed. There are no procedures in place to control this information once it leaves OIRM."	30
3.4.5.3: Sanitizing media for reuse	IRMS	"A device for sanitizing tapes and hard drives was available in Albuquerque, but it disappeared during the move to Reston. OIRM is considering purchasing another device. No formal procedures exist for sanitizing unused media or for its disposal."	31
	Reston LAN	"Not Applicable to the Reston LAN. There are no LAN devices that use magnetic media or flash cards. However, LAN supported servers and desktops do use many forms of magnetic media (e.g., hard disks, floppy disks, tapes, ZIP cartridges). Currently, there are no procedures for the disposal of such media."	31
3.4.5.4: Shredding hard-copy materials	IRMS	"Shredding of hardcopy takes place, but it varies among sites. There are no written procedures for shredding IRMS reports."	31
3.4.6.3: Following up on errors that cannot be immediately resolved	TAAMS	"No written procedures exist."	34
3.4.6.4: Data recovery procedures	IRMS	"No formal restoration procedures exist."	31
3.4.7.1: Procedures to protect sensitive data	BIANET	"There are no procedures in place."	38
	IRMS	"Formal procedures were not established yet."	31
	LRIS	"Currently, no such procedures exist."	44
	TAAMS	"Currently, no such procedures exist."	34

Section No. and Name	System	Problem Description	Page No.
3.4.7.3: Hardware inventory	BIANET	"There is no inventory control system for BIANET equipment. Equipment used by the BIANET is not under change control."	38
	TAAMS	"No formal inventory lists for TAAMS hardware and software exist."	34
	Reston LAN	"There is no inventory control system for Reston LAN. Equipment used by the Reston LAN is not under change control."	31
3.4.7.6: Disaster Recovery Plans	BIANET	"A Disaster Recovery Plan for BIANET was not developed. There are no current plans to develop one."	38
	IRMS	"A formal Disaster Recovery Plan for IRMS was not developed."	32
	Reston LAN	"A Disaster Recovery Plan for the Reston LAN was not developed. There are plans to develop one by the end of FY 2002."	32
3.4.7.8: Training employees for roles in emergency disaster and contingency plans	BIANET	"There are no training procedures or training curricula in place. When BIANET problems or disasters occur, OIRM personnel resolves them based on their knowledge of the network, prior experience, and the specific circumstances. ORIM personnel do not follow procedures when resolving BIANET problems, nor [do] such procedures exist."	38-39
	IRMS	"There are no training procedures or training curricula in place. When IRMS problems or disasters occur, OIRM personnel resolves them based on their knowledge of the network, prior experience, and the specific circumstances. ORIM personnel do not follow procedures when resolving IRMS problems, nor [do] such procedures exist."	32
	LRIS	"NBC/PS needs to develop a plan to ensure that all employees are trained in their roles and responsibilities relative to the emergency, disaster and contingency plans."	45
	TAAMS	"There are no training procedures or training curricula in place."	35

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"There are no training procedures or training curricula in place. When Reston LAN problems or disasters occur, OIRM personnel resolves them based on their knowledge of the network, prior experience, and the specific circumstances. OIRM personnel do not follow procedures when resolving Reston LAN problems, nor [do] such procedures exist."	32
3.4.7.10: Penetration testing	BIANET	"No procedures for penetration testing are in place. Except for a single test, which was performed in December 1999 on the Albuquerque router. The test revealed that the router had a weak password, which may allow intruders to easily access and modify router configuration. There are no written procedures for such tests and there is no schedule for performing these tests."	39
	IRMS	"No procedures for periodic penetration testing are in place."	32
	LRIS	"There is no penetration testing procedure."	46
	TAAMS	"As of the end of January 2001, no penetration tests were performed."	35
3.4.7.11: CFO Audits	BIANET	"There is no record of audit reports by the CFO."	39
	IRMS	"There is no record of audit reports by the CFO."	33
	LRIS	"There is no record of audit reports by the CFO."	46
	TAAMS	"There is no record of audit reports by the CFO."	35
	Reston LAN	"There is no record of audit reports by the CFO."	32
3.4.7.14: Recommendations in audits	BIANET	"Unknown."	39
	IRMS	"In the past only a few of the recommendation were implemented"	33
	LRIS	Unknown.	46
	TAAMS	Unknown	36
	Reston LAN	Unknown	32

Section No. and Name	System	Problem Description	Page No.
3.5.1.2: Procedures to ensure that maintenance doesn't affect security	BIANET	"There are no procedures in place to ensure that system security is not adversely affected as a result of maintenance and repair activities."	39
	IRMS	"There are no procedures in place to ensure that system security is not adversely affected as a result of maintenance and repair activities."	33
	TAAMS	"There are no procedures in place to ensure that system security is not adversely affected as a result of maintenance and repair activities."	36
	Reston LAN	"There are no procedures in place to ensure that system security is not adversely affected as a result of maintenance and repair activities."	33
3.5.1.4: Controlling remote maintenance	BIANET	"None. OIRM can use its network diagnostics and management tools to remotely monitor and reconfigure BIANET equipment. However, there are no written procedures that control such activities. OIRM personnel perform these tasks when needs and as they see fit."	40
	TAAMS	"No written procedures are in place."	36
	Reston LAN	"There is no remote maintenance for the Reston LAN."	33
3.5.1.5: Change management procedures	BIANET	"There is no change control and no change management procedures for the BIANET."	40
	IRMS	There is no change control and no change management procedures for the IRMS."	33
	Reston LAN	"There is no change control and no change management procedures for the Reston LAN."	33
3.5.1.7: Impact analysis	BIANET	"An official impact analysis for the BIANET was never performed."	40
	Reston LAN	"An official impact analysis for the Reston LAN was never performed."	33
3.5.1.8: Updating contingency plans	BIANET	"There are no contingency or disaster recovery plans. Since there are no plans, there are no updates as a result of changes in the BIANET environment."	40
	IRMS	"There are no contingency or disaster recovery plans. Since there are no plans, there are no updates as a result of changes in the IRMS environment."	34

Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"There are no contingency or disaster recovery plans associated with the Reston LAN. Since there are no plans, there is no need for updates as a result of changes in the Reston LAN environment."	33
3.5.2.1: Documenting software changes	BIANET	"OIRM does not have change control mechanisms to keep track of system software distributed in over 200 sites. OIRM does not maintain documentation for system software versions and changes."	40
	IRMS	"BIA does not have change control mechanism is place for Unisys system software."	34
	Reston LAN	"BIA uses COTS hardware and software components in Reston LAN equipment. OIRM does not have change control mechanisms to keep track of system software. OIRM does not maintain documentation for system software versions and changes."	34
3.5.2.2: Security tests for COTS software	BIANET	"There are no security test procedures for COTS software used in the BIANET."	41
	IRMS	"There are no security test procedures for COTS software used in IRMS."	34
	LRIS	"There are no written security test procedures for COTS software used in the LRIS architecture."	48
	TAAMS	"There are no written security test procedures for COTS software used in the TAAMS architecture."	37
	Reston LAN	"There are no security test procedures for COTS software used in the Reston LAN."	34
3.5.2.3: Control over personal id numbers, etc	BIANET	"No passwords are used to gain access to a router and viewing configuration information. Only account Ids are used. The router account ID is known to only three OIRM employees. Strong authentication is NOT used to access BIANET equipment."	41
	Reston LAN	"Account ID is the only control used to gain access to a router and viewing configuration information. Strong authentication is NOT used to access LAN or BIANET equipment."	34
3.5.2.4: Procedures to register and protect secrecy of passwords and log-on codes	BIANET	"No formal procedures were established. As was found in the penetration test, at least one router's password, in Albuquerque NM, was weak and easy to guess."	41
	LRIS	"No formal procedures have been established."	49

Section No. and Name	System	Problem Description	Page No.
	TAAMS	"No formal procedures have been established."	38
	Reston LAN	"No formal procedures were established."	34
3.5.2.6: Controls of back-door access	IRMS	"There are no formal controls"	35
	TAAMS	"Controls related to this 'back door' must be tightened."	38
3.5.2.7: Controlling activities of users and systems staff	IRMS	"Each user staff member is limited to individually-set subsets of the system. Less strict limitation apply to the system staff."	35
	Reston LAN	"No controls were implemented on the Reston LAN to monitor or control the activities of users and OIRM personnel within the system."	34
3.5.2.8: Separation of duties	IRMS	"No. Batch-balancing approaches are used. The controls are supplied by OTFM."	35
	LRIS	"In the NBC data center, critical functions are divided among different Branches and individuals whenever possible to provide separation of duties. Improvement needs to be made in the area of separation of duties in the testing and acceptance of system program changes in the mainframe environment prior to operational use."	49
	Reston LAN	"No controls were implemented."	34
3.5.3.3: Procedures for use of virus scanners	LRIS	"When a virus is detected, the user is notified and given the option to eliminate the virus."	50
	TAAMS	"When a virus is detected, the user is notified and given the option to eliminate the virus."	39
	Reston LAN	"There are no written procedures. OIRM configured the Virus protection software on every desktop computer and LAN server to execute automatically when the computer boots up. The software runs in the background and monitors files as they are copied onto hard disks on desktop computers or servers. LAN equipment, such as switches, do not use virus protection software. There are no written procedures for use of virus programs on the Reston LAN."	35
3.5.3.4: Scan and clean programs	IRMS	"The Norton AntiVirus program installed on every workstation allows users to scan floppy and hard disks for viruses, and if any are detected, to remove them."	35

Section No. and Name	System	Problem Description	Page No.
3.5.3.5: Instructions on cleaning systems	LRIS	"There are no written procedures that instruct employees how to remove viruses. Each site handles virus cleanup as specified by the local LAN Administrator."	50
	TAAMS	"There are no written procedures that instruct employees how to remove viruses. Each site handles virus cleanup as specified by the local LAN Administrator."	39
	Reston LAN	"There are no procedures to instruct Reston LAN users on how to check and clean their desktop computers."	25
3.5.4.2: Penetration testing	BIANET	"To date, there were no penetration tests targeting specifically the BIANET. Only one limited test was conducted on the Albuquerque router, which revealed deficiencies in securing the router, even against amateur attacks. There are no BIA policies and procedures for conducting penetration testing on BIANET equipment or over the BIANET."	42
	IRMS	"There are no BIA policies and procedures for conducting penetration testing on IRMS equipment or over the BIANET."	36
	LRIS	"There is no penetration testing procedure."	51
	TAAMS	"BIA approved and funded penetration testing on TAAMS. . . Continuing these test in the future will depend on the availability of funds."	39
	Reston LAN	"To date, there were no penetration tests targeting specifically the Reston LAN. There are no BIA policies and procedures for conducting penetration testing over the Reston LAN."	36
3.5.4.3: Message authentication procedures	BIANET	"BIANET routers can be configured to support encryption. However, in order not to adversely affect network performance, they are not. As a result, currently there are no procedures or mechanisms in place to ensure authentication of data transmitted over the BIANET. Furthermore, there are no mechanisms in place to ensure the authentication of remote management session of a router (e.g., telnet, or dial-up) because router management sessions are not encrypted either."	42
	LRIS	"Neither strong authentication nor encryption is currently used by LRIS."	51

	TAAMS	"Neither strong authentication or encryption is currently used by TAAMS."	40
Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"The Reston LAN does not use such procedures. There are no mechanisms on the Reston LAN to ensure the authentication and integrity of data transmitted over the LAN."	36
3.5.5.1: SAT for Execs. and Snr. Management	BIANET	"No security awareness training is in place for BIANET operators or OIRM personnel."	42
	IRMS	"No security awareness training is in place for IRMS operators or end users."	36
	LRIS	"No security awareness training is in place at the BIA."	51
	TAAMS	"No security awareness training is in place at the Service Bureau or the BIA."	40
	Reston LAN	"No security awareness training is in place for Reston LAN users or OIRM personnel."	36
3.5.5.2: SAT for Program and Function user managers	BIANET	"No security awareness training is in place and no requirements for the training courses were specified."	43
	IRMS	"No security awareness training is in place and no requirements for the training courses were specified."	36
	TAAMS	"No security awareness training is in place at the Service Bureau or the BIA."	40
	Reston LAN	"No security awareness training is in place and no requirements for the training courses were specified."	36
3.5.5.3: SAT for Information Resource Mngrs	BIANET	"No security awareness training is in place and no requirements for the training courses were specified."	43
	IRMS	"No security awareness training is in place and no requirements for the training courses were specified."	36
	TAAMS	"No security awareness training is in place at the Service Bureau or the BIA."	40
	Reston LAN	"No security awareness training is in place and no requirements for the training courses were specified."	36
3.5.5.4: SAT for end users	BIANET	"No security awareness training is in place and no requirements for the training courses were specified."	43

	IRMS	"No security awareness training is in place and no requirements for the training courses were specified."	36
Section No. and Name	System	Problem Description	Page No.
	TAAMS	"No security awareness training is in place at the Service Bureau or the BIA."	40
	Reston LAN	"No security awareness training is in place and no requirements for the training courses were specified."	36
3.5.5.5: SAT for contractors	BIANET	"No security awareness training is in place and no requirements for the training courses were specified."	43
	IRMS	"No security awareness training is in place and no requirements for the training courses were specified."	36
	TAAMS	"No security awareness training is in place at the Service Bureau or the BIA."	40
	Reston LAN	"No security awareness training is in place and no requirements for the training courses were specified."	36
3.5.5.6 - 3.5.5.: Coverage of SAT curricula	BIANET	"A security training curricula was not developed by BIA."	43
	IRMS	"A security training curricula was not developed by BIA."	36-37
	TAAMS	"A security training curriculum was not developed by the Service Bureau or the BIA."	40
	Reston LAN	"A security training curricula was not developed by BIA for the Reston LAN or for any of the systems directly connected to the Reston LAN."	37
4.1.1: Rules governing identification of system users and resources	BIANET	"There is no document describing the rules governing identification of BIANET users."	44
	IRMS	"There is no document describing the rules governing identification of IRMS users. . . . There are no documented procedures for user account management and disenrollment."	38
	LRIS	"There is no document that describes the rules governing identification of system users."	53

	TAAMS	"There is no document that describes the rules governing identification of system users.	42
Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"There is no document describing the rules governing identification of Reston LAN users. Since anyone with access to a workstation that is connected to the LAN automatically receives LAN connectivity to resources, special identification is not needed for general users. However, to use LAN resources, such as servers and printers, users must first log into the Novell server, which authenticates users prior to granting them access. There are no written rules that govern how users are identified and authenticated by the LAN."	38
4.1.2: Password rules	IRMS	"Currently, there are no written rules for password use for IRMS accounts."	38
	LRIS	"Currently, there are no written rules for LRIS account passwords established by BIA."	53-54
	TAAMS	"Currently, there are no written rules for TAAMS account passwords."	42
	Reston LAN	"Currently, there are no written rules for passwords used by Reston LAN users. However, there are rules that the LAN Administrator follows when managing users' accounts."	38
4.1.3: Rules for compromised passwords	BIANET	"No written procedures are in place for compromised passwords."	44
	IRMS	"No written procedures are in place for compromised passwords."	38
	LRIS	"No written procedures are in place for compromised passwords."	54
	TAAMS	"No written procedures are in place for compromised passwords."	42
	Reston LAN	"No written procedures are in place for compromised passwords."	38

4.1.4: Token controls [45]	BIANET	"None are used."	44
	IRMS	"None are used."	38
	LRIS	"None are used."	54
	TAAMS	"None are used."	42
Section No. and Name	System	Problem Description	Page No.
	Reston LAN	"None are used."	38
4.1.6: Controls securing remote access	BIANET	"No security policy is in place for remote access (via telnet or dial-up) to BIANET routers."	44
	IRMS	"No security policy is in place for remote access (dial-up is supported, telnet and Internet access are not supported) to IRMS. . . . No other controls, such as strong authentication, encryption, or secure tunneling, are used."	39
	TAAMS	"No security policy is in place for remote access. Access over dial up lines is not supported. However, access from the XXXX is supported. No written policies are available at this time, and no security controls, such as firewalls, are installed to reduce the risk of intrusion by remote access."	43
	Reston LAN	"The Reston LAN does not provide dial-up capabilities. All dial-up is accomplished via the Albuquerque RAS server. No security policy is in place for remote dial-up access to the BIANET and Reston LAN resources. Several LAN resources support XXXXXXXXXX, which can be accessed XXXXXXXX, however, there are no security policies to control such access either."	39
4.1.7: What controls are used for access to network routers and for secure data transmission	BIANET	"None of these approaches are currently in use."	45
	IRMS	"None of these approaches are currently in use. The only control used is simple authentication (a password). No additional controls were implemented to secure data transmission beyond defaults provided by COTS software. . . . No information is available whether passwords are transmitted as text."	39

[45] Tokens are objects, like smart cards, that a system user possesses for purposes of identification and authentication. See NIST Special Publication 800-12 at 184.

	TAAMS	"None of these approached are currently in use. The only controls used are basic authentication (User ID and password). No controls were implemented to secure data transmission beyond defaults provided by COTS software XXXXXXXXXXXX"	43
	Reston LAN	"None of these approaches are currently in use. The only controls used are simple authentication (a password). No additional controls were implemented to secure data transmission beyond defaults provided by COTS software (e.g., RAS security controls.)"	39
Section No. and Name	System	Problem Description	Page No.
4.1.8: Controls for securing dial-up communications.	BIANET	"The only control used on the RAS server is the account ID/password combination. OIRM issued around 1000 accounts. There are no written procedures in place to manage these accounts, e.g. close an account of a terminated employee."	45
4.1.9: Automated logoff	IRMS	"No."	39
	Reston LAN	"Some applications on the Reston LAN will terminate the connection to a desktop after a predetermined period of inactivity, or when the desktop is restarted. Reston LAN desktop computers use the Windows 98 operating system. Windows 98 supports protected screen savers. However, Windows 98 does not support passwords on the local computer."	39
4.1.10.: Self protection techniques	IRMS	"There is no password encryption during transmission from workstation to the Unisys NX. On the unisys, user ID and password files are encrypted. Unisys passwords are user-selected and can be modified by users at will. There is no dictionary to check to ensure that users do not choose passwords that can also be found in (conventional) dictionaries. The application password is assigned by OIRM and cannot be changed by end users."	39
	LRIS	"Passwords can be dictionary words. The system does not automatically disable accounts with weak or dictionary-words passwords."	56
	TAAMS	"These techniques are not currently used."	43
	Reston LAN	"LAN administrators are one of the Reston LAN groups. This group uses the same authentication techniques as any other group, namely, an account ID and a password. The same rules and techniques, used by any other LAN user, are used by members of the LAN administrator group."	39

4.1.11: Verifying default passwords are changed	IRMS	"No procedures for requiring default password changes are currently in place."	40
	TAAMS	"No procedures for requiring default password changes are currently in place."	43
	Reston LAN	"No procedures for requiring default password changes are currently in place."	39
Section No. and Name	System	Problem Description	Page No.
4.1.12: Does system use access scripts with embedded passwords	BIANET	"No."	45
	IRMS	"No."	40
	TAAMS	"No."	43
	Reston LAN	"No."	40
4.1.13: Does system use digital electronic signatures	BIANET	"No."	45
	IRMS	"No."	40
	LRIS	"No."	56
	TAAMS	"No."	43
	Reston LAN	"No."	43
4.2.2: Is network protected by firewalls?	BIANET	"No."	46
	IRMS	"No. OIRM is in the process of evaluating firewalls from various vendors. At this time funds are not available for this acquisition."	40
	LRIS	"The BIANET is not protected by Firewalls, but the Multiprise in the Denver data center is protected by a Cisco PIX firewall. The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available."	56-57
	TAAMS	"No. The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available."	44

	Reston LAN	"No. OIRM is in the process of evaluating firewalls from various vendors. As of yet no decision was made on which firewall to acquire and no funds are available for this acquisition."	40
4.2.3: Are network intrusion detection systems in place?	BIANET	"No."	46
Section No. and Name	System	Problem Description	Page No.
	IRMS	"No. No current plans for implementing intrusion detection systems on the Reston LAN and the BIANET due to the lack of funds."	40
	TAAMS	"No. The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available."	44
	Reston LAN	"No. No current plans for implementing intrusion detection systems on the BIANET."	40
4.3.1: Additional controls for public access	BIANET	"Information is not available."	46
	IRMS	"No firewalls are in place to mitigate intrusion risks from the Internet."	41
	TAAMS	"No firewalls or any other additional controls are in place to mitigate intrusion risks from the Internet."	44
	Reston LAN	"There is no public access to the Reston LAN and its resources, however, the LAN and its resources are visible to the public over the Internet. No firewalls are in place to mitigate intrusion risks from the Internet."	41
4.3.3: Audit trails	BIANET	"No logging for audit trails were implemented on the BIANET."	46
	IRMS	"No information is available to determine if and how auditing is configured on the Unisys NX and IRMS database."	41
	Reston LAN	"Logging for audit trails were implemented on some of the resources, such as the Unisys NX."	41
4.3.4: Ensuring system availability	BIANET	"The two security measures include physical security and account ID security."	46
	IRMS	"Only a minimal set of user access control is currently in place. It consists mainly of using account IDS and simple passwords to gain access to applications and databases, such as IRMS."	41

	TAAMS	"However, the use of security controls to ensure data availability on the XXXX is rudimentary. Only simple authentication is used to allow access to the system."	45
	Reston LAN	"The two security measures include physical security controls and environmental controls."	41
Section No. and Name	System	Problem Description	Page No.
4.3.5: Evaluations as to legal considerations	BIANET	"No such evaluations was ever conducted,"	46
	TAAMS	"No such evaluation was ever conducted."	45
	Reston LAN	"No such evaluation was ever conducted."	41
4.4.1: Audit trails for user action	LRIS	"No procedure for reviewing and analyzing the trails exist."	58
	TAAMS	"No procedure for reviewing and analyzing the trails exist."	45
	Reston LAN	"Audit trail facilities can be installed on LAN authenticating servers and application servers. . . . Reston LAN authentication servers do not use audit trails and no procedures for reviewing and analyzing the logs exist."	41
4.4.2: Ensuring audit trails record	LRIS	"No written procedures exist."	58
	TAAMS	"No written procedures exist."	45
	Reston LAN	"No such procedures exist."	41
4.4.3: Audit trails contain sufficient info?	IRMS	"There are no written procedures in place to ensure that audit trails were configured to correctly record sufficient and pertinent information."	42
	TAAMS	"There are no written procedures in place to ensure that audit trails were configured to correctly record sufficient and pertinent information."	45
	Reston LAN	"There are no procedures in place to ensure that audit trails were configured correctly to record sufficient and pertinent information."	42
4.4.4: "Restricting On-line Audit Logs"	Reston LAN	"Logs and audit trails were not implemented on Reston LAN authentication servers."	42
4.4.5: Audit trail review	TAAMS	"No written procedures exist. The system administrator reviews the logs periodically."	45

4.4.7: Who reviews audit trail following a known problem?	Reston LAN	"Audit trails were not implemented on Reston LAN authentication servers."	42
Section No. and Name	System	Problem Description	Page No.
4.5.1: Reviewing sign-in and sign-out logs for those with physical access to routers	LRIS	"No written procedures for reviewing sign-in and sign-out logs are currently in place."	59
	TAAMS	"No written procedures are currently in place."	46
	Reston LAN	"No such procedures are in place. Only a few individuals in the LAN administrator group have physical access to LAN servers, which are located inside the data center, and know the administrator's password."	42
4.5.2: Internal control audits	BIANET	"No such procedures are currently in place."	47
	TAAMS	"No written procedures are currently in place."	46
	Reston LAN	"No such procedures are currently in place."	42

SeNet also evaluated the physical security at the Addison, Texas and Reston, Virginia locations. Those reports revealed that:[46]

Section Name	Location & Draft	Problems	Page No.

[46] Two versions of the Physical Security Guidelines for the Addison, Texas facility were produced. The first, referred to herein as "Addison 1" lists a May 26, 2000 date on its cover page and a June 10, 2001 date on its interior pages. The second, referred to as "Addison 2" lists a June 16, 2000 date on both its cover and interior pages. Three versions of the Physical Security Guidelines for Reston, Virginia were produced. The first, referred to as "Reston 1" lists a February 17, 2000 date on its cover and a February 23, 2000 date on its interior pages. The second, referred to as "Reston 2" lists a February 25, 2000 date on its cover page and a March 2, 2001 date on its interior pages. The final version, referred to as "Reston 3" lists an August 4, 2000 date on both its cover and interior pages.

Sequence of Actions/Time line	Addison 1	"ATS has implemented several security controls, which greatly improved access control and intrusion prevention. However, the data center does not yet meet BIA's requirements for security."	6
Section Name	Location & Draft	Problems	Page No.
	Reston 1	"SeNet learned from Dan Marshall, ISI Senior VP responsible for the BIA contract, that currently there are no specific physical security plans for the building. . . . SeNet conducted a walk through the facility and inspected the proposed computer room and the existing security devices left behind by the previous tenant. After discussing the security issue with the Building Engineer Mr. John Hains of CarrAmerica our conclusion is that, currently, the only security measures for the new building are the existing door locks. That includes the main entrance door locks and interior door locks. There are no operational intrusion detection and alarm, systems in place. There are several motion detectors and CCTV cameras mounted to walls, but they are not operational and they are not connected to a central alarm/monitoring station."	4
	Reston 2	"Since the design, specification and implementation of a new security system may take weeks, it is possible that the computer room will become operational several months before the building is secured properly."	4
	Reston 3	"Under current plans, completion of the data center construction and the implementation of data center security measures implementation will coincide."	4

Facility	Addison 1	"The underground parking garages are open to the public 24 hours a day, but building management is considering installing garage door locks and key readers to prevent unauthorized parking. Building management is responsible for locking and unlocking main entrance and garage-level elevator doors. These doors are not protected by an alarm system. Like any other non-secure office building, there is no reception area or a guard in the main lobby. . . . Building management is not using the card reader system in the main entrance and in the parking garage to record or time stamp entries to the building. The card is used only as a key to open the door. . . . The building is not protected by an alarm system so if one of the entrance doors to the building is left open (intentionally or accidentally) it will not be detected until the next routine security inspection."	13
Section Name	Location & Draft	Problems	Page No.
	Reston 1	"The fact that the computer room floor is on the ground level, and the fact that sections of exterior walls and all exit doors are made of breakable glass, make this building vulnerable from physical security standpoint. . . . The rooms are 8-feet high with dropped ceiling. Between the dropped ceiling and the next floor there is a two feet open space, which spans the entire floor. An intruder could remove one of the ceiling tiles in an adjacent, unlocked room, and climb over the wall into the computer room. Both rooms have 2-inch solid core wooden doors. The AC room and Room A121 have locks. None have a cipher lock."	5
Recommendations/ Walls	Addison 1	"The TAAMS data center walls however are constructed from floor to ceiling only on the outside perimeter (North-South hallway and elevator shaft) of the room. Inside perimeter walls (walls facing ATS office-space) are constructed from floor to suspend ceiling, leaving a two-foot gap between the suspended ceiling and the third floor. Intruders gaining access to ATS office space on the North side can enter the data center through this gap."	16

Recommendations/ Doors	Addison 1	"All five entrance-doors, as well as the data center door that opens to the cubicles area, are equipped with proximity key readers and mechanical locks. However, the mechanical locks on all of these doors are not being used. Only the key readers and the magnetic locks are used to open and lock the doors."	17-19
Recommendations/ CCTV Recording System	Addison 1	"A CCTV recording system is used to record all entries and attempted entries into the data center. ATS did not install a CCTV recording system."	24-26

Finally, on July 15, 2001, published a Vulnerability Analysis of the IRM Ely Parker Building in Reston, Virginia. That report revealed that:

Problem	Relevant Language	Page No.
Authority over users	"Thousands of users in over 100 BIA sites use systems for which IRM is responsible, yet IRM has no authority over these users and cannot enforce security rules of behavior. Moreover, users of organizations other than the BIA (e.g., OTFM) may need access, sometimes privileged access, to BIA resources. In addition, non-BIA systems must be allowed to transfer and receive files to and from BIA resources. BIA has no authority over these users and the interconnected systems, and cannot control file containing Trust data once these files were transferred out of its resources to other systems. With such operational complexities, clear definitions of ownership, authorities and responsibilities in imperative for properly securing Trust data."	21
Lack of defined responsibility	"With no formal plans, responsibilities are assumed and relinquished on an ad-hoc basis."	22
	"For the most part, documented mission statements, delegation of authority and responsibilities, plans, policies and SOPs do not exist."	23

	"IRM data center personnel do not feel responsible for data center physical security or physical access."	24
	"[T]he CIO is also, 'on paper', the Acting Director of IRM. However, the CIO informed us that he was no longer acting as Director of IRM, while the Deputy Director, who left the BIA in mid-June 2001, informed us that he never assumed the role of the Director. This organizational quandary leaves the office of IRM without an effective leadership."	25
	"Lacking the necessary authority, BIA IT security officers are not in a position to enforce security policies at the field locations, and cannot unilaterally modify security controls on the Unisys NX to improve the security of Trust data."	26
Physical Security	"Data center physical security controls do not meet basic requirements (e.g., the duress systems in the data center does not work properly. In case of an armed break-in, data center staff will bot be able to notify the local guards or the remote monitoring station. The CCTV system does not work when there is a utility power outage. An emergency exit door is not alarmed and is not monitored by a CCTV.)"	24
Problem	Relevant Language	Page No.
Security Officer concerns	"The BIA Security Officer who is responsible for operating security controls and whose office is 15 miles away in Washington, D.C. claims that NBC did not adhere to mandatory BIA physical security requirements and will not formally accept the security system in the data center."	24
	"Officially, the BIA Security Officer and her designees (i.e., the guards) have responsibility for the operating of the data center physical security controls. However, the CCTV monitor and the records for the data center cameras are located in the offices of the IRM IT Security Group, which the guards cannot enter. Therefore, the IT security group was assigned the responsibility for changing the tapes. The group has no other data center CCTV-related responsibilities, which means they were not assigned the task of watching the monitor (they are sitting with their backs to the monitor). Practically, no one is watching this monitor, day or night, which raises the question of what the purpose of this monitor is. In comparison, the building's other CCTV cameras are connected to a monitor located on the guards' desk, which is being watched continually, day and night, by the guards."	27

Personnel Problems	"From a security standpoint, the adverse working environment, the lack of cooperation in transferring knowledge, and the fact that many long-term employees opted out, are very significant. Because of what appears to be unstructured, undisciplined, and undocumented practices in the Albuquerque office, institutional knowledge resided in employees memory rather than documents, such as plans, policies, procedures, design documents, listings, and software configuration. This institutional knowledge was lost with the resignation of most employees. Even in cases where documents existed, the resigning employees were not eager to tell the newly hired technical staff whether the documents were current or accurate."	29
Structure of Facility	"The extensive use of glass and natural light gives the building an open feel but makes it vulnerable from a physical security standpoint."	31
Problem	Relevant Language	Page No.
	"Physical access to both soft and hard copies of sensitive Trust data located in the programmers work area is unrestricted. Anyone (e.g., visitors) who gains access beyond the main lobby on the first floor can enter the programmers open work area. . . . If an intruder gains physical access to a programmers' workstation it is relatively easy to circumvent the XXXXXXXX and boot the machine. Once the workstation is booted, intruders can easily view or copy any file on the workstation."	40
	"The reviewed engineering drawings did not contain sufficient detail to indicate that the required two-hour fire separation for mechanical, UPS and Magnetic Recorded Media Storage areas were implemented."	47
	"The BIA router is physically located in the data center. It resides in a rack with no door to secure it. BIA does not control access to the data center. Therefore an unauthorized BIA or non-BIA employee could physically access the router if they can access the data center."	79
Policies & Procedures	"No policies or operating procedures exist to guide the help desk in routine activities."	33

	"No policies or operating procedures to guide schedulers in routine activities exist."	34
	"There are no policies and procedures to guide the Operators in daily activities."	34
	"The BIA Security Officer, or its designees (e.g., the guards), are responsible for the operations of all physical controls in the Ely Parker Building. Replacing tapes in the CCTV records, issuing ID badges, issuing card keys, and reviewing card reader logs are examples of physical control operations. The BIA Security Officer does not have a documented policy and procedure manual for physical control operations. Such document is needed to provide detailed instructions on how to operate and effectively utilize available security controls."	37
	"There are no written backup policy and procedures for the backup process."	41
Problem	Relevant Language	Page No.
	"Currently, there are no rules of behavior for IRM staff or for end-users. The most critical component, which must be implemented without delays, is password management. IRM cannot enforce password policies on users. Current password guidance provided by IRM are not strong or specific enough. A more detailed and enforceable password policy is needed. Based on our knowledge of embedded passwords in scripts (all are short dictionary words), user passwords are probably weak too."	90
	"IRM does not have a policy or procedures for patching or upgrading the operating system. This is an ad hoc process."	95
	"There is no change control process. Each application has one programmer who is responsible for implementing changes and controlling the application's configuration. In reality, other privileged users can modify production code without consultation with IRM. Changes to production programs are made without proper justification, notification, or documentation. Since auditing is not enabled, there is no trace of who performed these unauthorized activities."	95

	"IRM does not have a policy or procedures in place for capacity planning, performance monitoring, hardware baseline configuration control, or hardware change control. This is an ad hoc process."	95
Visitor Access	"The different levels of security requirements may create security problems. For example, IRM may want all visitors in the building to be escorted out by their host at the end of the visit. NBC, with less stringent security requirements, may let their visitors leave unescorted."	36
	"On several occasions we observed unescorted visitors in the hallways. Some were trying to get into the IRM office space by tailgating IRM employees. Since employees do not challenge unfamiliar employees, or visitors, a change of visitor policy for all building tenants requiring hosts to escort visitors out at the end of a visit is needed."	36
External Security Concerns	"Packages are neither x-rayed nor 'sniffed' by explosives detection equipment."	48
	"The parking is not controlled by any means. There are thirteen light poles located throughout the parking lots. Light levels were not evaluated at this time."	48
Problem	Relevant Language	Page No.
	"The exterior of the building is not provided with security lighting. There are recessed 'high-hat' high-pressure sodium lights in some of the soffit areas, however, these do not constitute security lighting and are not tied into the emergency power system. In addition, ground floor intrusion detection is essentially non-existent."	49
	"There is also a video intercom system installed at the entrance to the Data Center that allows communication with visitors. The intercom does not control the Data Center doors. Some perimeter doors are equipped with magnetic switches but intrusion alarms are not monitored in real-time due to current technical restrictions in ACS and IDS Systems."	49
	"There is no integration between the CCTV system and the monitoring system. Therefore there is no camera call-up on alarm or duress."	56

	"The North Courtyard entrance is not protected. A large vehicle (e.g., pick-up truck) can be loaded with explosives and driven into the courtyard area. This could destroy most of the building, and specifically the Data Center that is located adjacent to the courtyard."	57
	"Access to the loading dock, located on the north side of the facility, adjacent to the Data Center, is not protected. Vehicle or personnel access to the docks is unrestricted. The loading dock handles a wide range of cargo and large deliveries. A large truck (containing explosives) can be parked in this area and destroy a large portion of the building, and specifically the adjacent Data Center and UPS room."	57
Computer Access	"System for maximum unsuccessful logins "does not lockout the usercode that attempted to logon. XXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXX."	60
	"The default authentication mechanism within the NX system is to transmit the usercode and password in clear text. For more secure authentication, the NX supports Kerberos security features."	64
	"Prior to June 11, 2001, the BIA had implemented the maximum number of logon attempts and set this number to eight. As of June 11, 2001 this number was reduced to three. After three unsuccessful logon attempts, the station is locked."	66
Problem	Relevant Language	Page No.
	"Although BIA is assigning a unique usercode and password per user, because XXXXX is not installed and therefore the XXXXXX option is not enabled, all privileged usercodes have access to the XXXXXXXXXXXXXX. This type of access can be used to compromise user accounts. Therefore, BIA Security has little control over how usercodes are created and assigned access rights."	66
	"User Ids and passwords [for Oil & Gas] are hard coded into the application for each region. Therefore, all users in each region share the same application user ID and password used to logon. This makes auditing and tracking impossible. Because the user IDs and passwords are hard coded into the application, a separated BIA employee no longer authorized to access BIA resources will still know the correct user ID and passwords to access the application."	69

	"Application user IDs and passwords are stored on PCs. The PCs are physically secured because they are located in the data center, but they are accessible from the Internet. If the PC operating system is not secure, a malicious attacker could access the user IDs and passwords."	70
	"During processing, the user IDs and passwords are printed out on paper to be used by the operators. The hard copy printouts containing IDS and passwords must be disposed of properly, otherwise an unauthorized user could gain access. However, the court order prohibits the destruction of any Trust data related documents."	70
	"Because the BIA does not enforce a policy of least privilege for usercode access rights, [the Lease Range Nightly Processing] could be compromised by a malicious user or accidentally."	71
	"Because the *Range* master file is a flat file, any usercode with privileged permission can delete or modify the file with a simple ASCII text editor."	71
	"*LRIS* and *Osage* Trust data are downloaded into the programmers' workstation, which are Windows 98 machines. Trust data may reside on these machines overnight. Because the programmers are located in a non-secure area, and because it is fairly simple for an intruder to gain access to these machines, Trust data are at the risk of theft, destruction, or modification."	74
Problem	Relevant Language	Page No.
	"Currently, the Unisys maintains active privileged user accounts for employees who have departed the BIA several years ago, some who are deceased. IRM is hesitant to disable these accounts because no one knows who is using them and for what purpose. Disabling such an account may disrupt operations if the account was originally set up to perform a system function, such as transferring a file to another mainframe. Without documentation or institutional knowledge, the only way to find out the purpose of such accounts is to disable the account and see what happens, a risk that the management does not want to take."	74

	Number of Security Admin users at BIA as of 4/30/01: 10 Recommended number of users: 2 Number of System Users at BIA as of 4/30/01: 67 Recommended number of users: 5 Number of Privileged Users at BIA as of 4/30/01: 170 Recommended number of users: Never more than 1% Non-Privileged Users at BIA as of 4/30/01: 3000 Recommended number of users: "The BIA is in the process of removing several hundred, if not thousands, of default usercodes no longer authorized to access the system. The number of valid usercodes is unknown at this time."	75
Problem	Relevant Language	Page No.
	"As of April 30, 2001 approximately 170 usercodes have been identified as having privileges permissions. This greatly exceeds accepted security standards and is a serious security violation. A user with privileged permissions and Read/Write application permissions has full access to the daily transaction files for all usercodes. Transactions can be modified or deleted by privileged usercodes."	76

	"As of April 30, 2001 approximately 3000 usercodes have been identified as having default permissions. It has been estimated that only approximately 500 of these usercodes are valid users. The additional 2500 or so usercodes must be deleted because they can be used to compromise the system with little chance of auditing the actual user."	76
	"End users and their supervisors are notified via e-mail when a usercode is created. The e-mail message contains the new usercode and initial password. There is no control on the Unisys NX that forces users to change the initial password upon login. However, users have the ability to change their password at will."	77
	"There is no formal process for modifying Unisys NX or application user account privileges. If a user needs additional privileges, e-mail message from the supervisor to the IT Security group is required. However, if users no longer need a privilege, supervisors are expected to notify the IRM IT Security Office. That rarely happens."	77
	"There is no formal process for disabling Unisys NX or application user accounts. As a result, thousands of users have active accounts that are not needed any longer."	77
	"There is no formal process for deleting Unisys NX or application user accounts."	78
System Backups	"Unfortunately, system backups are not being performed. The BIA lacks the equipment to perform system backups. The current workaround for this problem is to manually synchronize users home directories between both Novell servers. Because this is a manual process, the data in user home directories for each server will never by fully synchronized. The Novell servers are not on a Universal Power Supply (UPS). If power were unexpectedly terminated, the servers could crash, possibly resulting in a loss of data."	85
Problem	Relevant Language	Page No.

Segregation of Duties	"Segregation of duties in the area of software configuration management does not exist. The same individual with privileged rights develops programs, test them, enters them into the Production Pack, executes them, and then removes them from the configuration. Such programs can manipulate Trust data for financial gain without leaving a trace. Currently, the purpose of about 20 percent of the programs is not understood by the operation personnel. IRM does not have a baseline software configuration, change control process, version control, or configuration management function for the Unisys NX. Privileged users modify programs and modify the configuration at will without documenting their activities."	89
	"Privileged users can circumvent the concept of segregation of duties in other areas. For example, privileged users can create other privileged and non-privileged accounts. The process for establishing new accounts is based on the concept of segregation of duties. It requires approvals from supervisors, regional directors, the BIA Personnel Security Office, and the IRM IT Security group before a new account can be established. The likelihood for collusion in such a process is extremely low. However, hundreds of privileged users can circumvent the process by directly creating new accounts, using these accounts for fraudulent activities and then removing the accounts from the system."	89
Auditing	"Both the XXXXXXXXXXXX and XXXXXXXXXX XXXX provide extensive auditing capabilities. However, auditing on the operating system level and on the application level are not utilized. The DMS database management system is not used, so the applications cannot take advantage of the extensive set of security controls it has to offer. Several times in the past few months programers tried to determine who removed Trust data files from the system but were unable because auditing was turned off. During the course of the Reston security study auditing was turned back on. The system administrator insists that operating system level auditing was always turned on. No regular periodic review of logs, including security logs, is performed. The IRM IT security group was under the assumption that auditing was not enabled and was surprised to find out that the security log was turned on. The IT security group has sufficient privileges to turn on auditing and manage the logs, but does not have the expertise to do it. It is likely that IRM has not reviewed security logs (or any other logs) on the Unisys for years."	91
Problem	Relevant Language	Page No.

	"Auditing at the application level does not exist. A transaction file is a collection of records generated by one agency without specification of the data entry user who entered the data. Applications for some agencies allow only one user at a time to enter records into the transaction file. Other agencies allow multiple users to enter records simultaneously. Some applications (e.g., *Oil and Gas*) require all users to use the same account ID and password, so even if auditing (wt the application level) was implemented, it would be meaningless because tracking a user would be impossible, There are no procedures for reviewing audit logs. Auditing can be easily defeated by hundreds of privileged users who can turn auditing on and off as they please, delete audit log files, or modify them."	91
Disaster Plans	"There are no formal [Disaster Recovery Plans and Procedures.]"	91
System Documentation	"System documentation is lacking significantly. As a result of the move, and perhaps during the years before the move, system documentation did not receive the needed attention. Many documents are missing, and some programs are not properly commented. About 20% of the programs are not yet understood. Recreating documentation for an application the size of IRMS is a very large project, estimated by IRM at $.5M."	95
Penetration Testing	"Our penetration activities went mostly undetected, except the initial scan that was reported to us by the BIA Information Security Manager Mr. Curran. There is no firewall or intrusion detection system in Reston. The only device to prevent and log penetration activity as the Cisco border router. The router is logging certain events, but these logs are not reviewed regularly, and they are set to overwrite automatically once it reaches a certain size."	98
	"Reston router package filter access lists allows access to all internal BIA IP address. Therefore, a compromised machine anywhere on the BIANet could be used to access a Reston resource. Although it was not within the scope of this test, SeNet found extremely vulnerable and compromised machines outside of the Reston network."	98

2. **SeNet International Reports: Recommendations**

In the BIA IT Risk Assessment Report and the Vulnerability Analysis of the Ely Parker Building SeNet recommends that Interior/BIA/OIRM:

1. "[P]rotect the network perimeter with strategically located firewalls, begin utilizing encrypted tunnels (VPNs), and introduce means of strong authentication." SeNet International: Information Technology Risk Assessment, Security Survey Report (January 4, 2001) at 8.

2. "To increase the visibility of security issues and strengthen the authority, [elevate] the information security function should . . . in the organization to report to the BIA CIO." Id. at 8.

3. Evaluate and recommend "new technologies; [and initiate] periodic evaluation of information security posture by conducting security audits and risk assessments." Id. at 8-9.

4. "Develop an application sensitivity classification standard and related procedure." Id. at 9.

5. "Classify all major applications and general support systems relative to the sensitivity of data." Id. at 9.

6. "Make adjustments reflecting this classification in Information Security Policies and Procedures." Id. at 9.

7. "Develop security awareness training curriculum." Id. at 9.

8. "Conduct mandatory awareness training as a part of initial employee orientation and at least once a year afterwards ('refresher' courses)." Id. at 9.

9. "Conduct mandatory security policies and technology training for the OIRM technical staff." Id. at 9.

10. "Develop and implement DRP test procedures for each of major applications and general support systems." Id. at 10.

11. "Develop and enforce Bureau-wide policy requiring strong passwords and their periodic change." Id. at 11.

12. "Consider other means of strong authentication, such as smart cards in conjunction with PKI."[47] Id. at 11.

13. "Establish on-line (electronic) Access Request Form utilizing digital certificates, and make appropriate process modifications." Id. at 11.

14. "Establish security-related Service Levels with each outsourcing service provider." Id. at 11.

15. "Add an entry on the form indicating the user's clearance status and level. Access privileges may be limited, permanently or temporarily, depending on this information." Id. at 11.

16. "Establish and enforce security related personnel policies and corresponding procedures including mandatory notifications of terminations and transfers." Id. at 11.

17. "Develop operational standards and provide specific training for system administrators to increase knowledge and awareness." Id. at 12.

18. "Set up a technical forum for system administrators. This forum (e.g. a mailing list, bulletin board, monthly meeting/conference calls etc.) will allow the exchange of information, address security concerns and develop/refine security operational procedures." Id. at 12.

19. "Create and publish Data Backup and Restoration Manual." Id. at 12.

20. "Implement off-site storage for LAN servers." Id. at 12.

21. "Design and implement a system of firewalls which will be used to establish 'Trust Zones.' Examples of such Trust Zones may include Regional Offices, Agencies, Data Center, OIRM LAN, etc." Id. at 13.

22. "Develop a Bureau policy for consistent mandatory use of virus detection and removal software on all workstations and servers." Id. at 13.

---

[47] "PKI" is an abbreviation for Public Key Infrastructure. PKI utilizes "certificate authority (CA), which issues digital certificates that authenticate people and organizations. *TechEncyclopedia* <http://www.techweb.com/encyclopedia/defineterm?term=PKI> (Visited Nov. 9, 2001).

23. "Develop and implement a procedure for regular updating of virus data files." Id. at 13.

24. "Develop a well thought through Bureau policy specifying acceptable use of Internet and e-mail, balancing business needs with employee's privacy." Id. at 13.

25. "Evaluate, select and implement a consistent means of contents monitoring and filtering." Id. at 13.

26. "Make employees aware of the policy, enforcement measures and consequences of non-compliance." Id. at 14.

27. "Enforce the policy." Id. at 14.

28. "Establish encrypted tunnels (VPNs) between major BIA user locations." Id. at 14.

29. "Deploy secure client software on portable user workstations and at smaller offices (agencies) and use encryption on dial-up connections." Id. at 14.

30. "To simplify administration and take advantage of common infrastructure components, consider establishing BIA-wide public key infrastructure, including BIA Certificate Authority." Id. at 14.

31. "Develop and adopt a procedure to address this risk." Id. at 14.

32. "Augment monitoring and reporting capabilities with additional tools to make the process simpler and more efficient." Id. at 14.

33. "Develop definitions of information security related incidents." Id. at 15.

34. "Develop and implement procedures for responding to such incidents." Id. at 15.

35. "Train appropriate personnel in the use of incident response procedures." Id. at 15.

36. "Develop and approve the BIA Information Security Policies document covering all aspects of information protection." Id. at 15.

37. "Develop and implement Information Security Procedures Manual based on the policies." Id. at 15.

38. "Conduct continuous awareness training program." Id. at 15.

39. Evaluate "all interconnected resources, users groups, and sites is requires to determine the true vulnerability of Trust data in the Ely Parker Building." SeNet International: Vulnerability Analysis: IRM Ely Parker Building, Reston, VA (July 15, 2001) at 101.

40. Conduct "[a] risk analysis of BIA operations in the Ely Parker Building." Id. at 101.

41. "[I]nvestigate common business practices and data manipulation capabilities of privileged users." Id. at 101.

42. "[C]ommission a study to compare its IRM budget and staffing levels to similar size organizations. One DOI agency (e.g., MMS) and one non-DOI agency (e.g., Indian Heath Services of HHS) are examples of agencies that may be used in the study." Id. at 101.

43. "[C]ommission a study to determine workload assigned to each of its current and recommended new staff positions. The study shall identify competency level requirements, daily tasks, and tasks duration to formally justify the need to increase budgets and staff." Id. at 101.

44. "[D]esignate one office with overall authority and responsibility over all security aspects of IRM IT operations. This office shall have the proper funding for ensuring adequate security controls for all BIA IT operations as mandated by Government regulations. Alternatively, DOI shall define the roles and responsibilities of the various security offices within the department and its agencies so that they do not overlap or contradict each other, and that no security gaps are created." Id. at 101-102.

45. "[S]pecify how agencies should interact when dealing with inter-agency security issues. DOI shall provide guidelines for determining which agency shall be designated as the leading security authority when two or more agencies/bureaus are cooperating on a joint project." Id. at 102.

46. "[D]evelop a meaningful organizational chart and mission statements clearly identifying the chain of command, responsibilities and authorities." Id. at 102.

47. "[R]eview position descriptions to verify accurate descriptions of duties, eliminating overlaps or gaps." Id. at 102.

48. "[D]esign data center physical security controls to support effective operations and management." Id. at 102.

49. "[D]evelop and publish a Security Incident Handling Policy and corresponding procedures, specifying who is responsible for handling the various types of security incidents within the Reston facility." Id. at 102.

50. Inform "[a]ll employees at the Reston facility . . . about the assignment of security responsibilities. This assignment shall be documented in the policy manual. Specifically, all IRM employees shall receive security awareness training that will identify the Reston facility focal point for reporting security incidents." Id. at 102.

51. "[D]evelop and publish a policy for regional offices and agencies specifying security requirements for accessing and the use of IRM computing resources. The policy shall specify who has the authority to enforce security policies and procedures in the field offices, and the focal point for reporting security incidents." Id. at 102-103.

52. Rewrite "[p]osition descriptions for security-related positions . . . so that they reflect the organization's mission and so that they do not conflict or overlap with each other." Id. at 103.

53. Clearly specify in "[t]he position description . . . the qualification and competence level required to successfully fulfill the position duties as specified in the position description. It may be required to reassign or train existing personnel, or to hire new personnel to meet position's requirements for security related positions." Id. at 103.

54. "[I]dentify areas of expertise in the field of IT security mandatory for securing its operations in the Ely Parker Building. Examples of such areas include: Unisys NX security controls, determining minimum privileges levels for end-users, assigning privileges to Unisys NX users, using InfoGuard security features, using legacy application security features, Lotus notes security, Desktop security, communication equipment security controls, etc. BIA shall ensure (by training, hiring or contracting) that it possess the expertise needed for effective security operations." Id. at 103.

55. "[D]evelop a master plan identifying and defining the scope of documents needed to formulate security plans, policies, processes, and procedures and shall be responsible for developing them. The IRM shall inform the Office of the CIO which documented plans, policies, procedures, and processes it requires to ensure secure IT operations in the Ely Parker Building." Id. at 103.

56. "The Albuquerque Software Configuration Manager is on the BIA's payroll. [T]ask the Manager with rebuilding configuration management for the Reston Unisys." Id. at 104.

57. "[P]lace higher priority on deciphering and documenting software modules." Id. at 104.

58. "[E]stablish a mechanism that will allow only an applications's designated programmer and the configuration manager access to software modules." Id. at 104.

59. "Complete control over card keys allowing access into the data center and IRM facilities shall be assigned to IRM." Id. at 104.

60. Allocate "[a] physically secured space shall . . . to include all IRM employees and contractors who display, store or print Trust data." Id. at 104.

61. Establish "[a] field account management function . . . to effectively manage the Unisys user community. Account managers shall have the technical knowledge and proper automated tools needed for effective control of system level and application level accounts." Id. at 104.

62. "[A]nalyze the tasks performed by end users and determine the minimal level of privileges required for each job category. IRM shall acquire and install the tools that allow the assignment of minimal set of privileges to users. IRM shall review each and every active and valid Unisys account and assign to it the minimal set of privileges." Id. at 104.

63. Modify "[t]he Computer Access Request (CAR) form . . . to include requests for various privilege levels." Id. at 104.

64. "[I]nstitute processes, policies and procedures for enrollment and disenrollment, and specifically mandate field offices to report to IRM employees' terminations and transfers." Id. at 104-105.

65. "[D]evelop a safety and security policy manual for the Ely parker building, acceptable to both organizations." Id. at 105.

66. Delegate "[r]esponsibility for managing and maintaining data center physical security controls . . . to an on-site IRM employee." Id. at 105.

67. "[D]evelop a procedure requiring data center staff to conduct a beginning-of-day check of all data center security controls. A checklist shall be created and used to indicate the operational status of each control. The on-site BIA employee designated as the data center physical security officer shall review the checklist on a daily basis." Id. at 105.

68. Limit to OIRM "full and exclusive control over physical access to the Unisys room. No other organization shall have control over assigning physical access to this room." Id. at 105.

69. "[D]evelop policies and procedures for physical access into the data center and into the Unisys room." Id. at 105.

70. "[D]evelop a plan for implementing available, optional, and third party IT security controls for all its IT resources, including networking gear." Id. at 105.

71. "[D]evelop the necessary documentation and provide step by step operational instructions for managing and operating physical security controls in the facility." Id. at 105.

72. "[E]valuate the effectiveness of fraud detection mechanisms on the Trust data systems, and the possibility for a single, privileged individual to manipulate data without being detected." Id. at 105-106.

73. "[D]evelop a policy and procedures for its privileged users regarding access to Transaction and Master files." Id. at 106.

74. Document and evaluate "[f]ield business processes, in particular the Interface process, . . . from a security standpoint. The evaluation shall determine the possibility of misuse by data entry personnel." Id. at 106.

75. "[R]elocate to a secured zone that will provide physical protection for Trust data." Id. at 106.

76. Forbid programmers from "keep[ing] lists of User IDs and passwords (files or hard copies) in their work area. The only location where hard copies containing account IDs and passwords may be kept is inside the data center. After hours, such hard copies must be placed in a safe." Id. at 106.

77. Forbid programmers from "keep[ing] Trust data files on their hard disks or on removable media (e.g., floppies). IRM shall create a home directory for each programmer on the departmental server (which is housed inside the data center). IRM shall configure security access on home directories to allow Read, Write, Modify, and Delete operations only to the users." Id. at 106.

78. Upgrade "[p]rogrammers' workstations . . . to Windows 2000. IRM shall develop and enforce a security configuration policy for W2K workstations." Id. at 106.

79. Reengineer,"in consultation with MMS and OTFM, . . . the file transfer process for files containing Trust data to ensure secure transfers." Id. at 106.

80. "[R]estrict access to the directory containing the MMS file only to the Gas & Oil programmer and individuals at the system administrator level." Id. at 107.

81. "[D]ocument its backup policy and procedures and shall address procedures for destroying failed or obsolete media containing Trust data." Id. at 107.

82. "[E]stablish a physically secured area where Trust data reports and other hard copy materials can be stored. An acceptable solution can be a file cabinet inside the data center." Id. at 107.

83. Restore "[d]irect communication . . . and [install] local alarms at the guard's station so that duress and alarms can be responded to immediately. The system's engineering design should be upgraded to minimize the risk of defeat. Finally, advanced features should be integrated to enhance the level of security that is required at the BIA Data Center. A longer-term solution to the security system upgrade would be include an advanced multi-site security management, under government control, that will facilitate enterprise-level security of the BIA Data Center, the building security, and other related/connected facilities. Such a system would allow the BIA Security managers to maintain central control of their entire integrated security system, while allowing regional offices to maintain independence and autonomous operations of their respective regional security systems." Id. at 107.

84. "[S]pecify and implement a ground floor intrusion detection system that is capable of detecting unauthorized access, CCTV surveillance and assessments, automatic call-up of alarm-associated camera outputs, pre and post alarm recording of camera outputs." Id. at 107.

85. "Upgrade the CCTV System for additional camera inputs, with advanced surveillance and assessment capabilities; Provide digital recording capabilities that facilitate advanced storage, retrieval and event search capabilities; Provide integration with the ACS, IDS and Duress system components; Allow for remote call-up by authorized monitoring personnel; [and] Connect the system to UPS power." Id. at 108.

86. Perform "[a] risk . . . to evaluate auxiliary mechanisms for reporting alarms to public safety authorities." Id. at 108.

87. "[B]lock access to the courtyard by placing large, heavy, planters at the entrance, or any other means." Id. at 108.

88. "[L]imit access to the loading dock by means of a gate and/or barrier, controlled by the guards, and/or authorized building personnel." Id. at 108.

89. "[I]nstall security lighting around the facility with emergency power backup." Id. at 108.

90. "[V]erify that the doors, frames and related hardware meet the requirements of heavy duty, high security specification that is suitable to the BIA Data Center." Id. at 108.

91. "[C]ontrol facility parking including an ID system for authorized parking. Post signs and arrange for towing unauthorized vehicles." Id. at 108.

92. "[E]nsure adequate lighting is provided for parking areas with emergency power backup." Id. at 108.

93. "[I]mplement x-ray screening for all UPS, FEDEX and other packages, including visitors' packages." Id. at 109.

94. "[V]erify with the Authority Having Jurisdiction (AHJ) that indeed the work has been performed according to local codes." Id. at 109.

95. "[I]nstall emergency power off switch as specified by the code." Id. at 109.

96. "Develop system schematics and equipment descriptions for the existing ACS, IDS, Duress and CCTV headends and installed devices; Document all new and replacement security devices in engineering documents; Develop a configuration management database documenting characteristics for all headend and building equipment; Implement a facilities management software program (Visual Information Management System) to assist in documenting and managing the configuration of the security system; Document the system specifications; Prepare as-built drawing; [and] Prepare a 'test plan' describing procedures to be used to test the system." Id. at 109.

97. "[C]onduct the test to be sure that every component operates as specified under various conditions." Id. at 109.

98. "[P]repare a written Fire Emergency Plan, a Security Plan, OEPs and contingency procedures including bomb threat procedures. Provide training and exercise with tenants. Establish law enforcement agency/security liaisons. Review/establish procedure for intelligence receipt and dissemination. Establish uniform security/threat nomenclature. Finally, conduct annual security awareness training." Id. at 109-110.

99. "[E]valuate the level of risk, quantify the level of protection that is provided by the UPS system, and determine whether additional lightning protection provisions are required." Id. at 110.

100. "[E]valuate the level of risk and prepare the following: A program to protect the records in accordance with their importance; Analysis of the workload and its effect upon continuity of operations; A written set of requirements for the backup site including Backup files and equipment required, Configuration of mainframe computer and peripheral units, Alternate locations for backup processing, Availability of backup systems, Telecommunications required at backup site, Files, input work, special forms,

etc. needed, Personnel staffing and transportation, Agreements and procedures for emergency use of computer equipment at a contingency site." Id. at 110.

101. "[I]nstall XXXXX security enhancement software and activate the XXXXXX option." Id. at 110.

102. "[U]se XXXXXX to assign additional granulated privileges to default user accounts to provide the least level of access necessary to perform a particular job." Id. at 110.

103. "[I]nitiate log backup and review and internal auditing. The security logs should only be accessible to a security administrator. The logs should be backed up and stored offsite for future audits and investigations." Id. at 111.

104. "[I]mplement appropriate file ACLs (Access Control Lists) using guard files to protect sensitive data." Id. at 111.

105. "[I]nstall virus and Trojan protection software." Id. at 111.

106. Review "[u]sercode attributes . . . to verify they meet the Unisys recommendations for highly secure system." Id. at 111.

107. "[D]ecrease the number of users with privileged permissions as recommended in the NX Operating System Security section." Id. at 111.

108. Reengineer "[a]ll applications containing hard coded user authentication information should . . . to allow for a unique set of credentials to be entered for each user." Id. at 111.

109. Do not store "[u]ser IDs and passwords . . . on PCs. The default configuration of a PC is insecure, making it feasible for a malicious internal user (and external user if the machine is connected to the Internet) to gain access and obtain this information." Id. at 111.

110. Document "[e]ach application and the programs that make up the application." Id. at 111.

111. Institute "[c]onfiguration management and change control . . . to test and document all modifications to application configuration." Id. at 111.

112. Migrate "[t]he Osage application . . . to a more secure and robust database solution." Id. at 112.

113. Limit " the ability to manipulate production data when data entry errors occur" to "trusted operators." Id. at 112.

114. Install "[s]ystem edits . . . to prevent duplicate files from being processed. In the current environment, a file previously processed could be inserted in the NX and run as if it were a new file." Id. at 112.

115. "[R]eevaluate and remove unnecessary privileged usercode permission as this is the most significant security hole within the NX system. When properly configured, the default, or non-privileged, user permission is sufficient for performing most user activities. When appropriate, use InfoGuard granulated permissions to provide users access to system resources otherwise inaccessible to the default usercode." Id. at 112.

116. "[I]nstall InfoGuard security enhancement software and activate all of the password security options, such as maximum and minimum password length, password aging, and number of password generations." Id. at 112.

117. "[D]ecrease the number of maximum logon attempts from 10 to 3." Id. at 112.

118. "[C]reate a usercode naming convention to assist in determining the resources accessing the system. The naming convention shall include a combination of specific information, such as region, username, workstation, etc. that would make user identification easier and provide for more granularity when audition user activity." Id. at 112.

119. "[I]dentify and delete all inactive usercodes. Separated employees could gain access using inactive usercodes that have not be [sic] removed. Accessing the system using inactive usercodes would make user identification very difficult." Id. at 113.

120. "[R]eview the logs files and audit successful and failed user logins on a daily basis. BIA shall install XXXXX to ensure that only the Security Administrator has access to the security logs." Id. at 113.

121. Change the default password for "[t]he XXXXX . . . to something that is compliant with current password conventions." Id. at 113.

122. Move "the router . . . located in the data center . . . to a location that is only accessible by authorized BIA personnel or a new rack with a locking door shall be installed." Id. at 113.

123. "[D]esign and implement a comprehensive boundary protection architecture that includes firewalls, VPNs, intrusion detection tools, virus protection and content filtering. Until a firewall is installed and properly configured, the router access lists should be

modified to prevent unnecessary BIA IP addresses from accessing Reston network resources." Id. at 113.

124. Disable "[t]he HTTP access to the router from the Internet . . . ." Install SSL "if HTTP is necessary for remote configuration, to encrypt authentication information." Consider "using a secure transmission method such as SSH if the router is being accessed from outside the BIANet." Id. at 113-114.

125. Disable "XXXXXXXXXX. . . on all hosts until a firewall is installed and properly configured." Id. at 114.

126. Consult "the BIA legal counsel to ensure the warning banner displays all necessary information that would hot hinder prosecution." Id. at 114.

127. Do not use "[t]he XXXX default settings shipped with the XXXX switches." Id. at 114.

128. Enable "MAC address port-level security on all switches . . . to limit the number of workstation that can attempt a connection to the switch." Id. at 114.

129. "[C]onsider allowing contractors to have home directories on network servers where Trust data can be safely temporarily stored." Id. at 114.

130. "Consider using proactive tools like Crack to test user password strength." Id. at 114.

131. Complete recent purchase of "equipment to enable system backups and to attach the servers to a UPS system." Id. at 114.

132. "[R]eview the [DOI Standards for Local Are Networks] checklist and make system modifications that would assure compliance with this list." Id. at 114.

133. "[E]stablish an email acceptable use policy that explains the use of BIA email, use of encryption for sensitive data, misuse policy, etc." Id. at 116.

134. "[D]ocument the Notes system configuration, PKI, ACLs, and other security related information." Id. at 116.

135. "[U]pgrade all XXX servers running on XXXXXXXXX to 128 bit service pack 6a immediately." Id. at 116.

136. "[I]nstall SSL on the Notes server to support encryption of remote user authentication and data." Id. at 116.

137. "[R]emove all services on the NT.W2K servers that are not used." Id. at 117.

138. "[D]evelop and implement a process to disable accounts of separated users immediately following the personnel action." Id. at 117.

139. "[R]elease without delays the password management section of the Rules of Behavior to all BIA and contractor sites. IRM shall finalize the complete set of Rules of Behavior and formally release it to all sites." Id. at 117.

140. "[G]ive IRM the authority to enforce the Rules of Behavior and Acceptable Use Policies at the regional offices." Page Id. at 117.

141. "[O]btain a password cracker for the Unisys password file. Periodically, the IRM IT Security officer shall attempt to crack passwords in the file. The accounts with weak passwords shall be disabled until a new stronger password is created by the user." Page Id. at 117.

142. "[V]erify that all default account Ids and passwords have ben removed or disabled." Id. at 117.

143. "[R]edesign programs and scripts to eliminate the use of embedded account Ids and passwords." Id. at 117.

144. "[D]evelop a security awareness training program for all users. IRM shall develop the curricula for training at two levels: mangers and staff. The program shall provide trainers, training manuals. Training shall be mandatory at least once a year." Id. at 117.

145. "[D]evelop a security awareness training program for IRM employees. A special curriculum shall be developed for staff with system administrator rights to IRM IT systems." Id. at 117.

146. "[D]evelop a new user security orientation manual. The manual shall be given to all new users (employees and contractors) on the first day of employment at the BIA." Id. at 118.

147. "[D]evelop a security incident reporting and investigating procedure." Id. at 118.

148. "[R]eengineer and implement a comprehensive auditing function on the Unisys NX. IRM shall develop policies and procedures for managing and viewing the logs. IRM shall give only select group of employees the privilege to view or manage the system logs." Id. at 118.

149. "[D]evelop a Disaster Recovery Plan." Id. at 118.

150. "[D]evelop Disaster Recovery Procedures." Id. at 118.

151. "[U]pdate its Continuity of Operations Plan (COOP)." Id. at 118.

152. "[I]nstall a standby generator capable of supporting all data center systems, including AC and alarm systems. To eliminate time restrictions, the generator shall provide the capability of refueling while in operation." Id. at 118.

153. "[D]evelop a standard operating procedures manual for the data center. Procedures such as planned shut down, emergency shut down, user notification, and data center evacuation shall be included." Id. at 118.

154. Ensure that "[t]he data center [has] equipment and supplies necessary to contain minor water leaks. A wet/dry vacuum, paper towels, rags, and plastic sheeting can come in handy. Operations in the data center shall not be disrupted due to minor water leaks." Id. at 118.

155. "[D]evelop a safety manual for the data center." Id. at 118.

156. [I]mmediately address the servers identified to be compromised, as well as those others that were found to have potential vulnerabilities. Servers should be brought up to the latest software patch level, and 'hardened.'" Id. at 118-119.

157. "[M]odify its network architecture to reflect industry best practices, such as employing proven security strategy and infrastructure like OS/Application hardening, IETF RFC 1918 IP addressing, screened subnets, and De-Militarized Zones." Id. at 119.

158. Protect "[t]he Reston facility . . . from other BIA networks in order to limit and contain the scope of potential damage related to malicious activity or other incidents." Id. at 119.

159. Limit "DNS zone transfers . . . to only those hosts which have a business need to know internal addresses/names, and reverse lookups should be disabled for all but dedicated machines running necessary services (i.e., www, ftp, DNS, smtp, etc.)." Id. at 119.

160. Use "'split DNS' and Firewall De-Militarized Zones (DMZ) . . . . A split DNS is where dedicated external DNS hosts, dedicated internal DNS hosts, and strong security infrastructure are built to separate name resolution for their respective zones (public and private). This service should be password protected and proper ACLs created to restrict users to authorized directories." Id. at 119.

161. Disable "[a]ll open ports with no known purpose . . . on all hosts." Id. at 119.

162. Disable "file sharing shall . . . on all workstations." Page Id. at.

163. Explicitly prohibit "[s]toring Trust data on any workstation." Id. at 119.

F. Special Master's Site Visit Report

On March 12, 2001, the Special Master issued a report addressing the physical security of the OIRM Reston, Virginia facility. See Site Visit Report of the Special Master to The Office of Information Resource Management (March 12, 2001) ("Special Master's Site Visit Report").

1. Special Master's Site Visit Report: Findings

The Special Master's Site Visit Report revealed that:

(1) the Special Master was able to enter the facility via a construction entrance without identification (Special Master's Site Visit Report at 1); (2) a computer-generated printout labeled "Individual Indian Monies Interest Calculations" was lying on a shredder near the OIRM work space (id.); (3) the second floor of the facility could be accessed without a pass key or special identification (id. at 2); and (4) contractors admitted that trust documents may be left unguarded throughout the day (id. at 3).

G. Predictive Systems' Reports

On June 1, 2001, the Special Master engaged Predictive Systems ("Predictive")[48] to perform a vulnerability assessment of the DOI/BIA Internet Infrastructure in order to determine the overall security of the network segments and hosts within the scope of the engagement and to show whether it was possible to gain access to critical BIA systems and read, modify or delete the data contained on these systems.

To accomplish these tasks, Predictive proposed to conduct a penetration test in two phases: an external, Internet-based network testing phase to be followed by an onsite, internal network testing phase which would compromise critical hosts to gain access to trust data. This was unnecessary, however as, "[e]arly on in the testing it became apparent that it was possible to access the sensitive internal data from the Internet and that the internal on-site testing phase was not needed due to the lack of overall perimeter security of the BIA Internet Infrastructure." Predictive Systems Network Vulnerability Status Report of Bureau of Indian Affairs Trust Data Security ("Predictive Report") at 1.

In August 2001, Predictive issued a report focusing on the "potential vulnerabilities of the systems that belong to the Department of the Interior (DOI) Bureau of Indian Affairs (BIA) and methods for exploiting them." Predictive Systems Network Vulnerability Status Report of Bureau of Indian Affairs Trust Data Security at iii (August 2001).

1. **Predictive Systems Reports: Findings**

Between June 24, 2001 and July 8, 2001, Predictive performed an initial penetration test of systems identified by the BIA as being "critical" to their mission. As set out in the Predictive Report,

---

[48] Founded in 1995, Predictive is a network infrastructure consulting firm whose clients include the Department of Justice, the General Services Administration, the State of Michigan, the State of Massachusetts, the Virginia Department of Housing and Urban Development and the Virginia Department of Transportation, Chase Manhattan, Bear Stearns, Goldman Sachs, Credit Suisse/First Boston, Raytheon, Microsoft, Deutsche Bank, Pfizer, Mitsubishi, Solomon Smith Barney, Fidelity Investments, Comdisco, Citigroup, First Union, Freddie Mac and United Airlines. It also enjoys strategic alliances with SAIC, Cisco, BellSouth, Hewlett Packard, Tivoli, Micro Muse, Peregrine, RiverSoft, bmcsoftware and Compuware.

Predictive Systems was able to gain unauthorized access to both critical systems (IRMS and TAAMS) identified by BIA. Predictive achieved access to these systems that allowed creating shared directories, accessing data, and making changes to these systems (including adding user accounts). Predictive Systems was able to gain unauthorized access to these systems from the Internet using a variety of known exploits and openly available, freely downloadable software. While commercial tools and proprietary attack methods were used during this assessment, gaining access to the critical systems identified by BIA could be achieved by an attacker on the Internet using similar attack methods and freely available tools.

Predictive Report at v.

Specifically,

Problem	Page No.
Predictive was able to locate a list of users on the XXXXXXXXXXX server, determine the pattern for user names, and determine that the remote XXXX servers had a blank administrator password. Predictive was also able to access individual users' mailbox files.	9
By accessing the TAAMS XXXX through vulnerabilities on the BIANET (caused by blank administrator passwords) Predictive had "access to information such as all of the users that were allowed to access the database, database schema information, and even data stored in the database." Such information gave Predictive "access to view, change or modify any information available on the XXXX system."	9-11
Again utilizing weaknesses on the BIANET, Predictive gained access to the IRMS XXX XXXXXX-based administration software files. These tools enabled Predictive to "connect to the target system as an administrator without [the program] prompting for any form of authentication," giving Predictive "complete access to all user management functions on the XXXXXX system." Such access allowed Predictive "to see every account that existed on the XXXXX system. In addition, the user management program allowed full access (change, modify, delete, add) to the user database."	13
Predictive accessed a list of all user accounts and passwords found on one of the XXXX XXXX backup domain controllers.	14
Using a simple login and password, Predictive was able to log into the XXXXXXX system.	14
It was possible to login to the XXX Server (IRMS) by hopping through other vulnerable hosts on the BIA network. Once there, Predictive found that the administrator account had a blank password and was able to log into the system and obtain complete control of the server. From this point, it was possible to create Windows Networking shares, create users, and transfer files to and from the server.	24-25
Predictive was able to connect to the TAAMS system with no password which allowed it to obtain interactive access to the system as an administrator.	27

Predictive found that the Blank Admin Password on the XXX Server provided a low difficulty of exploitation: "Predictive was able to log into the system and obtain complete control of the server."	24-25
Predictive found that the Weak Admin Password on the XXXX Server provided a low difficulty of exploitation: "Predictive Systems had access to the XXXXXXXX application software available" on the server.	26
Predictive found that TAAMS XXXX Environment was compromised, leading to a low difficulty of exploitation: "Predictive Systems used this host to launch the majority of the attacks on the servers that BIA identified as sensitive systems."	27
Predictive found that the Blank Administrator Password on the XXX Field Office Server provided a low difficulty of exploitation: "This server housed several gigabytes of XXX XXX email for employees of the BIA that were staged at this specific site. Additionally, the server was also linked to all of the other XXX servers throughout the BIA."	28-29
Problem	Page No.
Predictive found that Administrative Access to the routers could be obtained, and that this provided a low difficulty of exploitation.	29
"Predictive Systems found that sensitive information was available on several of the BIA's XXXX web servers anonymously. This information included server configuration details, log files, and user address book information." Predictive found that the difficulty of exploitation for this weakness was low.	31
"Predictive Systems was able to connect to many XXXXX hosts as 'Administrator' without supplying a password. Because of this, Predictive Systems was able to map all shared drives and obtain full control of the system."	33
Predictive found vulnerabilities, including the availability to upload XXX, "a command that allows a user to connect remotely and get command line access to a XXXXX host," on the Microsoft XXX Servers, and found that there was a medium difficulty of exploiting these vulnerabilities.	33-34
Predictive found that several XX hosts allowed anonymous logins, and that the difficulty of exploitation was low.	35
Predictive was able to access XXXXXXXXXXXXXXXXXXXXXXXXX on the systems. According to Predictive, "[a]n attacker can use XXX to obtain valuable information about the machine, such as information on network devices and current open connections."	35-36
Predictive found that sensitive files are available through anonymous XX, and that [e]nabling anonymous XX means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks."	37
Predictive found that "A XX server was running" on a host, with a low difficulty of exploitation. Predictive states that "XXX allows file transfers, with no authentication."	38
"Predictive Systems found that some registry keys were writable by users who were not in the admin group. Some keys affect system security. A malicious user may be able to alter these keys to escalate privileges on a system."	39

Predictive found that a host has a XXXX named XXXXX installed in a web server. According to Predictive, "[t]his is dangerous for many reasons. A malicious user may use this vulnerability to place files on web server to perform additional exploits."	39
Predictive found that a number of hosts (which are possibly printers) "are running a XXX application with no password."	40-41
"Predictive Systems was able to establish a null (anonymous) session with various XXXXX target hosts during this assessment.	42
"Predictive Systems found that it is possible to force to XX server to connect to other hosts by using the XXX command. This problem allows an intruder to use affected host to scan other remote hosts, making the scans appear to originate from the affected host."	46
Problem	Page No.
"Predictive Systems found that services like XXXXXXXX were running on these systems. These services can be setup to run 'unauthenticated.' That means that a user on one system that has a valid login, can access another computer if the same account exists on the other server without authenticating."	46
"Predictive Systems found that these hosts were running standard XX services like XX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, etc. May XX services are susceptible to various security vulnerabilities. These include Denial of Service attacks, intelligence gathering, and often specific buffer overflows or exploits."	47

Predictive concluded that:

> the Bureau of Indian Affairs' network infrastructure has not implemented many basic security practices. Even if every security vulnerability identified in this report was corrected, BIA's overall lack of a secure network perimeter would still leave BIA exposed to additional risk. Furthermore, Predictive Systems recommends that the Bureau of Indian Affairs create security policies and standards that describe best security practices, and then implement them. . . . Establishing a secure network perimeter (through firewalls, intrusion detection and other technologies), mitigates the risk of future exploitation by minimizing access to BIA systems and monitoring the perimeter network for active signs of intrusion.

Predictive Report at 48.

During a meeting which took place following the issuance of the Predictive Report to discuss its finding related to BIA Security, OIRM Director Brian Bowker suggested that Predictive would not

have been able to penetrate the BIA's infrastructure had Bowker not, in essence, "turned over the keys to the store." The inference drawn by the Special Master was that BIA was maintaining that its computer systems were more secure than indicated by Predictive and that its findings should be tempered accordingly.

Concerned that Mr. Bowker's representation was being offered to discount the ease with which Predictive was able to penetrate the BIA's computer systems, on August 30, 2001, the Special Master commissioned Predictive to once again penetrate the BIA systems and, this time, create a false account in his name.

In October 2001, Predictive issued its second report reiterating the findings in its initial report that the Bureau's computer systems were vulnerable to outside attack – even when approached from a completely different network than that used in the first penetration test. Special Task Vulnerability Assessment Report For Bureau of Indian Affairs, October 2001 ("Second Predictive Report") at 5. Again, to emphasize "the poor state of implemented security measures on the Bureau of Indian Affairs Networks," Predictive "made it a point to use only free tools and utilities, which are widely available on the Internet," to penetrate the computer systems. Second Predictive Report at 1.

Once Predictive gained access, it targeted the XXXXX server in an attempt to alter the data on one of the XXXX and create an XXXXXXXXXXXXXXXXXXXXXXXX. Id. at 9. They were successful and altered XXXXX an existing XXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXX.[49]

The Second Predictive Report found that both are the BIA networks and the trust data housed

[49] XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

therein are vulnerable to attack. Specifically,

Problem	Page No.
It was possible to access the XXXXX server and perform functions with administrative privileges.	28
It was possible to control the computer remotely using the standard XXXX XXXXXXXX administration tool which allowed Predictive to stop and start services, edit registry keys, enumerate users, hardware configurations, etc.	28
XXXX was running as a service on this host which allows remote access to a computer terminal.	29
Problem	Page No.
It was possible to map the XXXXXX drives of this computer over the internet which allowed Predictive to upload files to and download files from this computer.	30
It was possible to access sensitive information about XXXX via the XXXXXX XXXX.	31

2. **Predictive Systems Reports: Recommendations**

The two Predictive reports urged the BIA to:

1. "Deploy firewalls to establish a secure network perimeter to protect the network, systems and data of BIA. From reviews of documents and interviews with SeNet Corporation, the BIA network will need anywhere from three to seven firewalls to provide minimal perimeter protection. The perimeter defenses will create zones-of-trust to isolate and protect critical BIA systems so that only applications permitted to access the systems is allowed. All other accesses will be denied, logged and reported." Network Vulnerability Status Report of Bureau of Indian Affairs Trust Data Security (August 2001) at 29.

2. "Deploy Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activity. The Intrusion Detection Systems can be set up to monitor the network perimeter and critical systems located on internal BIA networks. The IDS devices should be deployed in conjunction with the firewalls to monitor the secure perimeter and other key systems. Approximately three to ten IDS devices should be deployed." Id. at 49.

3. "Implement a monitoring and review capability to monitor firewall logs and intrusion detection events. The monitoring program, will serve to accomplish, at a minimum, the following: Identify evidence of prior compromise (identification of established Trojan horses/back doors); Identify evidence of new attack activity; Establish necessary services and traffic; Establish data access control and transfer methods; Assess

effectiveness of defenses; Identify unintended operational impact (e.g., blocking legitimate traffic)." Id. at 49.

4. "Update router configurations and ACLs based on a more thorough knowledge of the actual operating requirements. The current router-filtering scheme is incomplete and inadequate. There are a number of security improvements that can be made at the routers to provide an additional layer of security." Id. at 49-50.

5. "Conduct a review of the entire information security plan in effect at BIA. The plan, at a minimum, must address the guidelines identified in OMB Circular A-130, especially Appendix III, 'Security of Federal Automated Information Systems.'" Id. at 51.

6. "Develop appropriate security policies to provide guidelines for appropriate use, behavior and performance, enforcement and to start creating a culture of security awareness with the BIA. The foundation of all security is Policy. With policies to establish standards for performance, any security that is emplaced [sic] quickly weakens. Policy must be centrally controlled, mandated, and disseminated to all personnel." Id. at 51.

7. "Develop appropriate business continuity and disaster recovery plans for all critical BIA systems. Business Continuity and Disaster Recovery plans are the key to quick recovery from unforeseen events. They provide a set of procedures and instructions designed to guide personnel." Id. at 51.

8. "Deploy other defenses (VPNs) if BIA cannot be entirely contained with perimeter defenses. It may not be feasible or possible to entirely contain all sensitive information within these secure perimeters. The use of VPNs for remote access from individual users or satellite offices is a suitable alternative to deploying a full firewall/IDS solution in these instances." Id. at 51

9. "Design and deploy appropriate system hardening to all systems, both servers and workstations. Firewalls and IDSs provide excellent security, but are not sufficient on their own. Individual systems must be properly hardened to withstand attack, especially from insider-attacks. They must be regularly patched against known vulnerabilities, and monitored for unauthorized changes." Id. at 51

10. Implement "strong authentication mechanisms such as one time passwords." Special Task Vulnerability Assessment Report for Bureau of Indian Affairs (October 2001) at 28

11. Stop "running the remote computer management service." Id. at 29.

12. Stop "using XXXXXXXX (or any other) remote PC management tool, unless other, extremely strict access controls are in place to minimize the risk of compromise." Id. at

29.

13. Stop "sharing any directories, drives, or devices on a computer, unless extremely strict access controls are in place to minimize the risk of compromise." Id. at 30.

14. "[R]estrict[] access to [the XXXXXXXXXXXXX] Web server." Id. at 31.

15. "[A]pply the patch available from Microsoft to resolve [the Unicode exploit] vulnerability." Id. at 34.

16. "[U]pgrade to the latest version of Cisco's IOS. Predictive Systems also recommends not enabling the Web administration service on Cisco routers." Id. at 36.

VI. **CONCLUSION**

Nearly two years ago, the Court remarked that it was "alarmed and disturbed by the revelation that BIA had no security plan for the preservation of [trust] data . . . that BIA has now placed itself in the incredible position that it cannot now create such a plan with its own employees, but that it can do so only if this Court allows BIA to go forward with these government contractors creating the plan, and then insuring that this critical data is preserved and protected."

Hon. Royce C. Lamberth, April 4, 2000 Hearing at 11-12.

Today, nothing has changed. The critical data of concern to the Court remains housed on systems that have:

> no firewalls, no staff currently trained/capable of building and maintaining firewall devices, no hardware/software solution for monitoring network activity including but not limited to hacking, virus and worm notification. . . . [and] a serious lack of wide area networking and security personnel in general. The BIA is also far behind the other bureaus in Interior regarding staffing of messaging systems and infrastructure support. . . . There is currently no capacity for the OIRM to analyze daily system logs generated by the IRMS system to look for unusual or possibly nefarious activities or to track changes made to each data file. . . . . Likewise, there are insufficient current staff to handle to day to day configuration issues of the data communication wide area network (WAN) let alone monitor, log and report the increasing "hacking" type activity.

FY 2003 Budget Request to the Department Bureau of Indian Affairs Trust Reform – Information Resources Technology (COP), Statement of Problem/Current Condition.

After ten years of blistering reviews generated by federal agencies and private contractors, this deplorable condition is inexcusable.

It can not be argued that Interior was unaware of the hundreds of deficiencies and suggested remedies chronicled in this Report. See, e.g., July 2, 1999 E-Mail from David Shearer (Chief, IRM Program Planning Review & Standard Division) to numerous USGS, MMS, BLM, NBC, and BIA personnel (including a cc to Daryl White, Nancy Davis and a bcc to Information Resource Manager, Office of Trust Risk Management Robert McKenna (Subject: 1999 IT Security Workshop)) ("As you know, hackers continue to target the Federal IRM Community at an alarming rate."); April 10, 2000 E-Mail from IT Security Manager John Curran to IRM ADP COORDINATORS, RITSSPOCS ("The most serious security matter is that people can transfer files without a log being made of the transaction and the files may contain scripts, Trojan horses, viruses, or sensitive information that we don't want moving on our networks in this fashion. The hacking community is avidly working on the poor security of these programs looking for pathways into networks and host machines. We have no policy at this time on their use."); February 2, 2001 E-Mail from BIA Chief of Telecommunications Curtis Hohenstein to OIRM Deputy Director Ken Russell ("Currently 'Trust Data' is transversing [sic] the Bureau's Wide Area Network and is open to data theft from outside sources. Our entire Network is now 'open to the public' domain and is under constant threat of attack and includes ALL major BIA Applications and Operating Systems. The threat of crippling the entire BIANET is real.").

It also can not be argued that Interior was unaware that the manner in which it stores trust data violates public laws and federal regulations. See, April 4, 2000 E-Mail from OIRM IT Security Manager Steve Schmidt to DOI/ITSWG[50] (Subject: Department IT Security Plan) ("Our present IT security does not fully comply with existing public laws, federal regulations, and Executive Branch directions"); December 19, 2000 E-Mail from eGoverment Officer, Office of the CIO, BIA Paul Marsden to Special Assistant, Office of Trust Records, Office of the Director Pat Gerard, Dom Nessi

[50] Department of the Interior IT Security Working Group.

("The current state of IT security in the Bureau of Indian Affairs is tenuous and not in compliance with many federal statutes, regulations, or policies. This statement applies to the situation as of December 2000").[51]

Finally, it can not be argued that Interior was unaware of the desperate need for adequate funding to overhaul its IT Security program. It is a matter of record. When the Horn Subcommittee gave Interior the worst security rating in the Executive Branch, CIO Daryl White testified that the agency's "ability to completely implement an adequate computer security program" was "strongly dependent upon the availability of necessary resources." Computer Security Report Card at 156. This message was reinforced in a subsequent September 11, 2000 communication from Acting Director, OIRM William Pfancuff to DOI Bureau CIOs/Deputy CIOs (Subject: Weekly Highlights/IT Conference Status) which opined that the Horn Report Card, "perhaps in the long run . . . will serve to elevate awareness and funding/resources priorities this program so desperately needs." Indeed, Interior's abysmal rating prompted OIRM IT Security Manager Steve Schmidt to remark that the Horn Report Card "raised the awareness of computer security to the highest levels of Interior" and led to "[d]iscussions about the grade and the need for additional resources [being] personally communicated to the Deputy Secretary."). September 20, 2000 E-Mail from Steve Schmidt to ITSWG and OSPIR Managers. Schmidt speculated that security funding may be available since, "[o]n September 18, the Assistant Secretary for Policy, Management, and Budget signed a memorandum setting computer security as a priority issue and that computer security be made a first priority for allocation of remaining FY 2000 fiscal resources, wherever legitimate." Id. (emphasis added).

Mr. Schmidt's optimism was misplaced. As the record in this case has repeatedly proven, gestures such as drafting memoranda and communicating with Interior's senior management, without more, are without substance. Since IT Security became the topic of discussion in the highest levels of

---

[51] Beyond these concessions, as a matter of law, "[f]ederal employees are chargeable with knowledge of governing regulations or statutes." Doe v. Gates, 981 F.2d 1316, 1321 (D.C.Cir. 1993).

Interior and enjoyed the status of a "first priority," Indian trust data housed on Interior's computer systems remains unprotected.[52]

For example, the lack of firewalls and adequate perimeter security have been repeatedly identified by the OIG Reports and the SeNet Reports as among the most grievous risks threatening trust data. See, e.g., BIANet System Security Plan at 16 ("[b]ecause of the non-secure nature of the connection (e.g. no firewalls are installed) the BIANET and all the computing resources connected to it (e.g. BIANET' XXXX, IRMS' UNISYS NX, LRIS' IBM 3090) are extremely vulnerable to attacks over the Internet").[53] Notwithstanding, the BIA removed the firewalls from one of the only two

---

[52] As the underlying litigation has repeatedly dramatized, prioritizing trust reform efforts in an oft-intoned litany of Interior management. See, e.g., Testimony of former Assistant Secretary for Policy, Management and Budget, U.S. Department of the Interior ("Mr. Chairman, I can state unequivocally that these particular issues rank at the highest priority of the Department at this time") Misplaced Trust: The Bureau of Indian Affairs' Mismanagement of the Indian Trust Fund at 18; Testimony of former Secretary of the Interior Bruce Babbitt ("Because of the high priority of trust reform efforts, these resources were provided in anticipation of completion of a strategic plan that would meet the requirements of the Trust Reform Act") July 9, 1999 Trial Transcript at 3687; Testimony of Department of the Interior Deputy Assistant Secretary for Budget and Finance Robert Lamb ("the Department does acknowledge that a coherent, consistent approach to trust fund administration is essential to providing adequate service to account holders. We believe that this goal can be achieved within the Bureau of Indian Affairs by ensuring that a direct line of authority exists within the organizational structure of the Bureau. Currently, the Deputy Commissioner position possesses this line authority. We expect that this position will soon be filled on a permanent basis and assure you that Trust Funds and related trust asset reform efforts will continue to be a very high priority.") July 13, 1999 Trial Transcript at 4013; Testimony of George Gover "trust fund reform is [my] highest priority" and "the highest priority of Secretary Babbitt." June 18, 2001 Testimony at 1109.

[53] NIST considers firewalls to be critical components of an effective security system in that they,

> help[] implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be

locations where they were in use and the Office of the Solicitor now questions the prudence of allocating funds for their purchase. See May 29, 2001 E-Mail from Solicitor's Office Attorney Susan Offley to Department of Justice Attorney Phil Brooks, Solicitor's Office Attorney Sabrina McCarthy, (Subject Re: Cobell – Revised Response to Motion for TRO and Show Cause) ("Firewalls are not the biggest security risk in IRM at the moment. I don't want to telecast over email what is but it has been mentioned over and over again in all the meetings between DOJ attorneys and IRM staff and even with Toly."). Ms. Offley continues, "BIA is in the process of allocating substantial funding to cover the issues of biggest security concern for fiscal year 2001 and 2002. . . . I cannot say whether or not they can drum up more funding to cover the installation of firewalls or whether they would need to take the money away from those other, more significant concerns to fund a firewall project." Id. [54] What the agency does state with conviction, however, is that "it is not a good idea to suggest to the Special

---

> examined and evaluated. . . . . In a firewall-less environment, network security and all hosts must, in a sense, cooperate to achieve a uniformly high level of security. As mistakes and lapses in security become more common, break-ins occur not as the result of complex attacks, but because of simple errors in configuration and adequate passwords.

NIST Special Publication 800-10 at 15, 16.

[54] Apparently, the position of the Solicitor is not shared by the Department of Justice. See E-Mail from Susan Offley to Dom Nessi, Ken Russell, John Curran, Steve Schmidt, Sabrina McCarthy 5/29/01 Subject: Cobell – Revised Response to MO for TRO and Show Cause,

> After a meeting last Friday with Dom Nessi and Toly Kozushin of SeNet, Justice attorneys are of the mindset that BIA should institute firewalls right away. At that meeting, Toly represented that firewalls could be instituted in 2 weeks if appropriately funded. However, at last week's TMIP meeting, BIA stated that they needed $1.6 million to fund short term solutions, none of which include firewalls (from what I can tell). Instead, I believe the money for firewalls will come from the $1 million budget request for FY 02. We need to explain to Justice why this $1.6 million isn't going to firewalls and why we made the decision to wait until 2002 to begin instituting them.

Emphasis added. Presumably, this explanation will be shared with the Court as well.

Master that he force us to initiate firewalls when there may be bigger security risks out there that BIA is already scrambling to find funding to correct." Id.

Without evaluating the relative merits of the Solicitor's observation that "more significant concerns" or "bigger security risks" may exist than an adequate perimeter, it is apparent that, as late as May 29, 2001, the BIA was still "scrambling" to locate funds to correct deficiencies that have long threatened the safety of trust information and that have been underscored by every organization that has studied the problem.[55] See, e.g., OIG Report No. 97-I-196, Report of Independent Public Accountants on Internal Control Structure (December 39, 1996) at 37 ("We suggest that disaster recovery planning over the mainframe environment continue to a be a high priority for the Bureau. Our understanding is that the disaster recovery contract is currently up for bid and has been delayed pending government funding."); ("We recommend that the Assistant Secretary for Indian Affairs ensure that: (1) Sufficient staff are provided to adequately monitor all visitor activities; (2) Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room."); OIG Report No. 97-I-771, Audit Report: General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (April 30, 1997) at 24 ("We recommend that the Assistant Secretary for Indian Affairs ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility."). See also BIANET System Security Plan at

---

[55] The "scramble" for adequate funding must be evaluated in the light of testimony given two months earlier before the Subcommittee on Interior and Related Agencies. In his introduction, the Special Trustee noted that "[a]dditional funding has been appropriated each year for the day-to-day trust asset management program operations of the Bureau of Indian Affairs (BIA), Minerals Management Service (MMS), Bureau of Land Management (BLM) and the Office of Hearing and Appeals (OHA). Because of these additional resources, the Department has made progress in implementing much needed Indian trust reform efforts." Opening Statement of Thomas N. Slonaker Special Trustee For American Indians before the Subcommittee On Interior and Related Agencies Committee on Appropriations U.S. House of Representatives at 1. There is notably no mention in the Special Trustee's introductory testimony of Interior's IT Security concerns or of the need for additional resources to address these concerns.

18 ("OIRM is in the initial planning process for installing firewalls in the five BIANET hubs. Another firewall is planned for the TAAMS data center in Dallas, TX. Once funds are approved, OIRM will solicit requests for proposals for firewall acquisition and installation. Firewall rules will be available for after the firewalls are fully configured and tested. Virtual Private Networks (VPNs), Internet content filtering, and intrusion detection devices are also under consideration for implementation by OIRM during FY2002 (depending the availability of funds")); BIANET System Security Plan at 21-22 ("[B]ecause of lack of funding no special measures to ensure non-repudiation and data integrity were implemented by OIRM. . . . Currently, because of lack of funding, OIRM is not taking any proactive measures to increase the reliability and availability of BIANET equipment that is under its control."); Reston LAN System Security Plan at 17 ("BIA has not conducted a vulnerability and risk assessment of the Reston LAN. The assessment shall be conducted after funds are approved"); BIANET System Security Plan at 24 ("There are no current plans for a BIANET risk assessment. However, BIANET is a high priority effort for OIRM. It will be conducted as soon as funds become available."); BIANET System Security Plan at 24 ("A security audit was not conducted on any of the BIANET sites. No new BIANET node installations are planned. Security audits will be conducted as soon as funds become available."); BIANET System Security Plan at 25 ("For the lack of funding, [no security audit] scheduled at the present time"); BIANET System Security Plan at 31 ("When funding becomes available, OIRM plans to conduct a physical security survey of all BIA sites connected to the BIANET"); IRMS System Security Plan at 25 ("Is biometrics in place or planned? "No/Yes, when funding is available"); TAAMS System Security Plan at 39 ("BIA approved and funded penetration testing on TAAMS. . . Continuing these test in the future will depend on the availability of funds"); IRMS System Security Plan at 40 ("No. OIRM is in the process of evaluating firewalls from various vendors. At this time funds are not available for this acquisition"); LRIS System Security Plan at 56-57 ("The BIANET is not protected by Firewalls, but the Multiprise in the Denver data center is protected by a Cisco PIX firewall. The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available"); TAAMS System

Security Plan at 44 ("The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available"); Reston LAN System Security Plan at 40 ("OIRM is in the process of evaluating firewalls from various vendors. As of yet no decisions was made on which firewall to acquire and no funds are available for this acquisition"); IRMS System Security Plan at 40 ("No current plans for implementing intrusion detection systems on the Reston LAN and the BIANET due to the lack of funds"); TAAMS System Security Plan at 44 ("The BIA Information Security Program (presently under development) provides for the installation of firewalls, but funds are not currently available").

In truth, the system is in its current state of disrepair because protecting trust funds is not now, and has never been, a "priority" deserving of adequate resources.

In light of this deplorable record, certain questions must be answered.[56]

Why, for example, on June 15, 2001, after the publication of tens of thousand of pages detailing every conceivable problem challenging the agency's security systems, does DOI Chief Information Officer Daryl White wish to conduct yet another "review of the current state of Trust Management IT security across the Department[,] [b]ased on the results of [which], Interior will be prepared to make decisions on how to proceed with implementing IT security as part of the Trust Management program. . . ." Memorandum from Daryl White to Chairman, Trust Management Improvement Program (TMIP) Steering Committee. On that score, why, after the publication of 30 reports – the majority of which were generated at considerable expense to the Department – did the Office of the Special Trustee commission yet another report which intones the identical litany of problems that have long been a matter of record.[57]

---

[56] This list of questions is illustrative and not exhaustive.

[57] On November 7, 2001, Electronic Data Systems ("EDS") – at the behest of the Office of the Special Trustee – issued its "Recommendations: For Comments Report – Information Assurance" – purporting to address the agency's IT security deficiencies. Given the recent issuance of this report, it will not be commented on in depth except to note that it offers not one unique observation from

Why would the CIO – who is statutorily responsible for "providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency . . . ," 40 U.S.C. § 1401, not review the 18 SeNet reports he commissioned at the expense of nearly one million dollars.[58]

---

previously commissioned reports nor offers any original insights or recommendations. See, e.g., "Add firewalls to the BIANET" Id. at 8; "Immediately implement and enforce password management practices which comply with BIA requirements and industry standards." Id. at 10; "Restructure the ATS contract to adhere to regulatory, departmental and industry practices" Report at 11; "Review Federal, DOI, OST and BIA regulations and guidelines as well as industry practices." Id. If anything, the sparseness of detail in EDS' offerings is alarming considering the wealth of information which was at its disposal. And in those instances where EDS supplies clarification, its suggestions are noticeably shy of the particularity contained in the Andersen, OIG, SeNet and Predictive Reports. Given the near million dollars expended by the agency to commission the SeNet reports (and its exhaustive list of recommendations which went unheeded), it can only be hoped that not too much money was expended in securing this latest pale effort. What is not needed to rectify years of neglect is yet another restatement of the same problems in an effort to convince the Court that progress is being made.

[58] Special Master: And I guess maybe I should start now by asking before we do so, have you read the [SeNet] IRMS security plan?

Nessi: No, I have not.

Q Now that sort of strikes me as curious, sir. Why would you not read – didn't you contract with SeNet to perform certain studies on your behalf?

A Yeah, on the department's behalf. Absolutely.

* * * *

A You know, with all the duties that I have, I would not be able to get to each of them.

Q Have you read the [SeNet] LRIS report?

A No. I haven't read any.

June 14, 2001 Interview of Dominic Nessi at 50-52

Why, on June 12, 2000, was the CIO compelled to transmit a memorandum to Assistant Secretary Kevin Gover, Director, Office of Administration and Budget Deborah Maddox, BIA Deputy Commissioner for Indian Affairs Sharon Blackwell and Principal Deputy Trustee Thomas Thompson "[a]ttach[ing] a plea from the CIO's office requesting a yes vote on funding for the Interior Architecture project . . . . one of the four breaches" in an attempt to impress "that funding is still up in the air and should be a higher priority."

Why, in March 2001, did the Special Trustee, in his introduction before a congressional subcommittee, underscore Interior's "efforts and commitment to resolve decades of trust fund management issues for both Tribal and individual Indian account holders" yet make no reference to the February 9, 2001 Information Technology Security Program version 1.0 which described "systems and information stores that are readily subjected to unauthorized disclosure, non-approved modification, and lost availability," or to "[r]esultant losses to the Department includ[ing] a continuation of those risks already realized including resources consumed by court litigation, losses from financial fraud, loss of financial audit credibility, expenses for recovering from system compromises, unavailable IT services, and public embarrassment." Id. at 1.

Why, in response to the Special Master's query as to CIO Nessi's inability to raise adequate funds to support the trust architecture did Mr. Nessi respond, "People needed money for so many things that this did not raise – this did not rise to, in their minds, a higher priority."[59]

It is clear that, just as Mr. Nessi did not review the studies he commissioned on behalf of BIA, neither did any other Interior official. If they had, there would be little need to conduct yet another review, which "will contain recommendations for implementing an adequate IT security program for Trust Management system in the Department," Memorandum from Daryl White to Chairman, Trust Management Improvement Program (TMIP) Steering Committee or commission additional reports from third-party contractors such as EDS.

[59] Special Master: Who is they?
Nessi: I would say anybody who had input into the budget.

And, perhaps most significantly, why was the Court not informed – via the Quarterly Reports that Indian trust data was virtually unprotected.[60]

It appears clear that, had Mr. Nessi not publicly aired his frustration (and prompted the instant investigation), the problems described in this Report might never have surfaced.[61]

August 8, 2001 Interview of Dominic Nessi at 155.

Nessi, on that score, recalled, "saying [on July 5, 2000] to [Tom Slonaker, Tom Thompson and Office of the Special Trustee Budget Officer Dave Gilbert] that one of the areas – you know, I had been using TAAMS money to strengthen BIANET, security-wise, XXXX servers and those kinds of things. And I recall very specifically they told me they would rather I did not spend TAAMS money on what they considered to be IRM expenditures. . . . That I should not use TAAMS money, trust reform money to upgrade the BIANET; that that was not the responsibility of trust reform." August 8, 2001 Interview of Dominic Nessi at 164. Emphasis added.

[60] The agency was clearly cognizant of its responsibility to do so. See May 30, 2000 E-Mail from Associate Director for Water, US Geological Survey Rudolph Hirsch to Director, Office of Trust Responsibility Terry Virden, Contracting Officer, Office of the CIO, BIA Tammy Harris, Dom Nessi, Ken Russell, Dr Ryl, Steve Schmidt, BIA Y2K Project Manager Ed Socks

> As you know, the recent court procedures have resulted in a directive to BIA to strengthen its protection of the Indian Trust Funds, and to send quarterly reports to the court outlining activities undertaken and progress made in line with that directive. Our tasks in those activities include identifying and quantifying the risks and vulnerabilities currently associated with keeping and processing the Indian Trust Fund records, and creating system security plans for BIANET and LANS. Your inputs will be essential for this task, and therefore we will contact you soon to obtain information about those systems. I would appreciate a face-to-face meeting with your for this purpose.

Emphasis added.

[61] If the representations made to the Court in opposition the plaintiffs' request to enjoin the OIRM move from Albuquerque to Reston serve as any yardstick, there is no reason to expect that the agency will candidly inform the court of any untoward developments as they arise. See, e.g., March 21, 2000, Opposition to Plaintiffs' Motion for Preliminary Injunction at 14, 21, 32 and 37 (arguing, inter alia, that the contracts with ISI/PRT "fully comply with the law;" that plaintiffs have failed to demonstrate any irreparable harm; and that contractors needed immediate access to all OIRM systems "to avoid system failures and possible loss of [trust] data."); March 7, 2000 Declaration of Kevin Gover at ¶ 12 (staff at the Reston facility are "taking the necessary steps to protect trust information and

It is incomprehensible that those with input into the budget process were unaware that the BIA was "so short of resources [that it faced] a major system failure at some point in the next two years." Id. at 95. Government Executive, *Trail of Troubles*, April 2001 at 96. If the former Special Trustee Paul Homan is to be credited (and if the protection of trust data were truly a "priority") there should have been no such shortage of resources.

Gingold: In your experience at the Interior Department, Mr. Homan, if the Secretary

---

documents.") See also 3/16/00 Declaration of Edward Williams (Exec. VP - PRT) at 18 ("[o]nce permitted to complete the relocation plan, PRT expects a decrease in the risk of data corruption due to the improved data center, implementation of written procedures, and stabilization of staff. Every day of delay perpetuates a situation in which the data is less secure than it could be.");

Indeed, one of the cornerstones of defendants' argument in opposition was the existence of a System Operations Security Plan ("Security Plan") that would address, inter alia, "data security and transition phases . . . on-going data security management, including security access management," Opposition at 13 (emphasis added). According to this Security Plan, Phase One would revolve around the location and "the required tasks to preserve the present data integrity and environment," while Phase Two would "include[] implementing best practices in the area of IT Data and Operations Management, improving upon areas of critical deficiency, such as installing a firewall for security, and other improvements once the present environment is re-established, up and running." March 8, 2000 BIA Security Operations Plan at 1.0, p. 3 (emphasis added).

On March 22, 2000, defendants filed a Correction to Defendants' Opposition to Motion for Preliminary Injunction and Motion for Emergency Hearing informing the Court that there was not, in fact, a Security Plan and that their previous posture of compliance with OMB Circular A-130 was incorrect. Id. at 2. The lack of these plans, they argued, "add[ed] urgency to Defendants' request that PRT/ISI be allowed full access to OIRM systems immediately . . . [and] is additional evidence of the need for BIA to assert managerial control over OIRM." Id. at 3. Once the Court's approval was garnered, however, there was no longer a sense of "urgency." On November 30, 2000 – nine months later – defendants filed a Notice of filing of reports on Office of Information Resource Management, Bureau of Indian Affairs and TAAMS. Under the section entitled Information Technology Security, defendants stated, without detail, that "as of April 2000, OIRM operations were not in compliance with all required information technology ("IT") security requirements. There is still significant work to be done in this regard, but now that the new data center has been safely relocated, more effort can focus on long-term IT security matter." Emphasis added.

seeks funding for items that he regards as on his highest priority, does he ordinarily succeed in getting those funds?

Homan: Yes.

June 11, 1999 Trial Transcript at 349.

VII. **RECOMMENDATION**

Interior – in derogation of court order, common-law, and statutory and regulatory directives – has demonstrated a pattern of neglect that has threatened, and continues to threaten, the integrity of trust data upon which Indian beneficiaries depend. Rather than take any remedial action, its senior management has resorted to the condescending refrain that has consistently insinuated itself into the federal government's relationship with Native Americans, in general, and with IIM holders, in particular. And that is one that requests forbearance and trust on the grounds that reform continues to be the "highest priority." It is the view of the Special Master that, in this instance, such trust is not warranted, requests for forbearance should be denied and promises of future compliance should not be credited. The stakes are simply too high. An agency that ignores its own commissioned reports and those generated by other federal agencies; ignores pleas from its own staff for adequate funding; and spends tens of millions of dollars funding computer systems when the integrity of the very data to be loaded on those systems has been open to compromise for so many years, inspires little confidence.

The security of systems housing trust data is no better today than it was ten years ago. The circumstances leading to the Court's alarm "that BIA had no security plan for the preservation of [trust] data," Hon. Royce C. Lamberth, April 4, 2000 Hearing at 11, speak with compelling application today. The continued lack of trust data security is "vivid proof" that Interior has "still failed to make the kind of effort that they are going to be required to ever make trust reform a reality." Id. at 12. It is the recommendation of the Special Master that the Court intervene and assume direct oversight of those systems housing Indian trust data. Without such direct oversight, the threat to records crucial to the welfare of hundreds of thousands of IIM beneficiaries will continue unchecked.

Respectfully submitted,

_____

Alan Balaran
SPECIAL MASTER

DATE: _____